I.T.T. Sistemas de Telecomunicaciones

PROYECTO FIN DE CARRERA

Despliegue de una red IP/MPLS para un ISP

Autor: Jesús Díez Álvarez

Tutor: Manuel Urueña Pascual

Leganés (Madrid), Diciembre de 2015

Agradecimientos

A mis padres en primer lugar, por hacer de mí la persona que soy hoy, en la que gracias a ellos me he convertido. Por dar lo mejor de sí mismos intentando siempre que mi vida fuera si cabe más fácil, anteponiendo mi futuro, bienestar y felicidad a los suyos propios, por todo… y más... ¡gracias papá y mamá!

A mi hermano menor Sergio, porque aunque sea el "pitufo gruñón", siempre me ha apoyado y animado, a su manera, a seguir adelante, dejándome entrever su admiración y orgullo, el cual siempre ha sido y será mutuo. Y claro…. ¡Gracias por hacerme tío!

A mis abuelos, porque para mí siempre han sido mis segundos padres, y como tales se comportaron.

A mi abuela, a la que admiro por su fuerza de voluntad, entereza y perseverancia, que sólo con su ejemplo, aprendí a ser más fuerte. (Y a ti abuelo que aunque ya no estés, no pasa un día sin que te recuerde y eche de menos… gracias por tus historias, cuentos y anécdotas que me hicieron comprender lo que es la vida).

A mi "Gorda", simplemente por ser como eres. Porque no me imagino una vida en la que no estés tú a mi lado. Por tu apoyo en los momentos de bajón, por tu ánimo en los momentos de desesperanza, por tu ayuda siempre que la necesité, incluso cuando no la pedía. Por amarme, porque eso ha hecho que sea mejor persona, que quiera superarme en todos los aspectos de mi vida, con el único fin de mejorar nuestro futuro juntos. Y por último por tu paciencia, infinita… tan grande que hasta a veces me sorprende. Gracias mi vida.

A la "panda del moco", ese grupo que todo niño sueña con tener y que siendo adulto se ha convertido en una familia de amigos donde los problemas son de todos y los apoyos y las risas para superar los momentos complicados nunca faltan. Gracias chicos, ¡sois los mejores!

A los "topos", Noe, Jose (Getafe), Jose (Móstoles), Mari, Edu, Manu, Marquichuel, esos compañeros de universidad, que hacían que los días enteros en la biblioteca estudiando fueran más amenos y divertidos que un fin de semana. Gracias por vuestro apoyo, vuestros conocimientos, vuestros apuntes (sobre todo va por ti Noe), en definitiva, por vuestra ayuda…. ¡Sois muy grandes!

Y cómo no, gracias a mi tutor Manuel, que me ha guiado en la consecución de este PFC, aconsejándome y ayudándome en las dudas que han podido surgirme.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Resumen

En este PFC se pretende explicar de la forma más didáctica posible, el despliegue de un entorno de proveedor de interconexión de redes y servicios (ISP), desde el supuesto teórico de un proveedor de servicios portadores ficticio (AbstracTel S.A.), que decide invertir y dar el paso para crear una red de *Backbone* basada en tecnologías IP/MPLS (*Internet Protocol/Multiprotocol Label Switching*) para su posterior uso en la prestación de servicios corporativos a empresas, tales como VPNs (*Virtual Private Networks*) de niveles 2 y 3, VoIP (*Voice over IP*), conectividad a la Internet, redes de distribución de contenidos o incluso servicios de alojamiento y respaldo en la nube.

La elección de esta tecnología MPLS sobre IP no ha sido fortuita, sino que viene apoyada y sustentada en el hecho de que la mayor parte de ISPs (*Internet Service Providers*) a nivel global usan esta tecnología para alcanzar los requisitos/tratamientos que los, tan diversos y diferentes, flujos de tráfico (información) precisan. Se detallarán así, los aspectos y motivos relevantes de esta elección.

Es importante mencionar que los datos aquí expuestos en cuanto a costes, tiempos, etc. pueden no ajustarse a la realidad, ya que tienen únicamente como objetivo servir de ejemplo (ficticio), a modo de acercamiento didáctico, de un despliegue real.

Abstract

This PFC tries to explain in the most didactic possible, the deployment of an environment for an internet service provider (ISP), from the theoretical assumption of a fictitious carrier services provider (AbstracTel SA), who decides to invest and take the step to create a backbone network based on IP / MPLS technology for future use in providing corporate services to companies, such as VPNs (levels 2 and 3), VoIP, Internet connectivity, content delivery networks or even hosting services and cloud backup.

The choice of MPLS over IP has not been fortuitous, but is supported and sustained by the fact that most global ISPs use this technology to meet the requirements/treatments that theses diverse and different traffic flows (information) require. Aspects and relevant reasons for this choice are detailed.

It is noteworthy that the data presented here, in terms of cost, time, etc. they may not be realistic, as they are only intended to serve as example, for didactic approach, of an actual deployment.

Capítulo 1: Introducción

1.1 Presentación del caso

Hoy en día la globalización ha dado como fruto la interacción global. Ya no es sólo que seamos capaces de saber qué acontecimientos ocurren en Japón casi tan deprisa como podemos saber qué tiempo hará en Burgos el fin de semana (casi seguro que frío), sino que podemos interactuar con personas que viven en dichos lugares a través de las redes sociales, llamadas telefónicas o por videoconferencia, mensajería, etc. Se ha convertido en hábito y rutina para muchos de nosotros el verificar el correo personal, el estado de tus redes sociales o los mensajes recibidos, varias veces al día. Pero no sólo en el ámbito personal sino también en el ámbito profesional, verificamos el correo a diario, puesto que se ha adoptado como estándar de facto en las comunicaciones empresariales. Nos conectamos a un cliente de mensajería instantánea corporativo para interactuar con compañeros localizados en otras situaciones (o incluso dos plantas más abajo que la nuestra) y así agilizar las labores de comunicación. Es decir, la comunicación/interacción global, a día de hoy, es un "habito necesario" y la hemos ascendido a la categoría de "indispensable" tanto a nivel personal como a nivel empresarial.

Para hacer frente a estos cambios, en las formas de interacción (virtual) y de intercambio de información, tan indispensables para el desarrollo del negocio, tanto entre empleados como entre aplicaciones o inclusive en la relación con cliente, las empresas precisan de proveedores de interconexión de redes y servicios. Estos ISPs han de estar adaptados a los diversos y cambiantes entornos tecnológicos para prestar estos servicios de comunicación, muchos de ellos críticos para determinados clientes.

AbstracTel S.A. es una empresa privada dedicada a la prestación de servicios portadores dentro del sector de las Telecomunicaciones en España. Hasta el momento servía como proveedor de acceso y agregación en el área de la Comunidad de Madrid.

Ante su más que favorable balance durante los últimos dos años, la directiva ha decidido reinvertir gran parte de los beneficios en la ampliación de su nicho de mercado y pretende el despliegue de infraestructura de red basada en tecnología IP/MPLS para la futura venta de servicios finales (redes privadas virtuales a empresas para voz/datos) y servicios de valor añadido (acceso a contenidos multimedia alojados en la nube, copias de seguridad, etc.).

Para ello y como consecuencia de los buenos resultados que ha venido experimentando con dicho equipamiento, Abstractel S.A ha decidido confiar de nuevo en el despliegue de routers Alcatel-Lucent. Dentro del portfolio que oferta este fabricante, se ha decantado por el uso de sus enrutadores orientados a servicios, en concreto, su gama 7750 SR (Services Routers), normalmente utilizados como nodos de frontera y nodos de backbone, en arquitecturas MPLS.

Debido a que la empresa desea el despliegue progresivo y moderado de su *Backbone* de red IP/MPLS, ha decidido comenzar con la implementación de equipamiento que cubra

el área geográfica de la Comunidad de Madrid y alrededores, donde ya posee clientes a los que proporciona acceso y agregación a otros proveedores de servicios.

Su mayor preocupación se encuentra en la escalabilidad. Desea que la solución ofertada sea escalable en un futuro y con capacidad suficiente en caso de un incremento significativo del negocio. Como es de esperar en estos casos, el cliente demanda que la red esté protegida frente a errores y dotada de mecanismos de recuperación frente a fallos que puedan surgir en las interfaces de interconexión entre los nodos.

1.2 Objetivo

El objetivo principal de este proyecto es la creación de una red de *backbone* IP/MPLS para dicho proveedor de servicios, la empresa AbstracTel S.A., bajo los requisitos mencionados anteriormente y utilizando equipamiento del portfolio del fabricante Alcatel-Lucent.

1.3 Estructura del documento

El presente proyecto se haya dividido en capítulos, cada uno de los cuales tiene como objetivo definir una parte importante de nuestro despliegue tanto a nivel teórico como práctico.

El Capítulo 2 está destinado al estado del arte. En él se describirán los protocolos que usaremos en el despliegue de la red de *backbone*, así como su funcionamiento en los equipos elegidos.

El Capítulo 3 ofrece una presentación del equipamiento y de los componentes escogidos en la solución, además de una breve descripción de sus características más destacables en relación al despliegue propuesto.

En el Capítulo 4 abordaremos aspectos relativos al diseño y la arquitectura escogida así como los detalles de su implementación y la configuración que se llevará a cabo en los equipos para el desarrollo de la solución.

El Capítulo 5 explica lo concerniente al presupuesto y la planificación de trabajo, detallándose las tareas principales del proyecto, los costes de recursos tecnológicos y humanos, así como los asociados a cada actividad.

Durante el Capítulo 6 llegaremos a las conclusiones derivadas del desarrollo del proyecto y a la presentación de los trabajos que en un futuro puedan desarrollarse para la mejora de la solución propuesta en esta memoria.

Finalmente se presenta un repositorio bibliográfico con aquellos documentos mencionados, referenciados o consultados durante la elaboración de este proyecto.

Capítulo 2: Estado del arte

2.1 *Multiprotocol Label Swtiching* (MPLS)

MPLS, acrónimo del término inglés *Multiprotocol Label Switching*, es una tecnología de conmutación de etiquetas que combina las capacidades de ingeniería de tráfico que ofrecen protocolos legados como ATM (*Asynchronous Transfer Mode*) o FR (*Frame Relay*) con la escalabilidad y flexibilidad que ofrece el protocolo IP (*Internet Protocol*).

De esta forma, MPLS brinda la posibilidad de establecer caminos orientados a conexión, a modo de circuitos virtuales, sobre la base de una red IP (en la que el protocolo IP es por definición no orientado a conexión).

Aunque desarrollaremos tanto las bases como muchos de los detalles de MPLS durante la implementación de la red IP/MPLS que este PFC tiene como objetivo, puede afirmarse que la esencia del protocolo MPLS es permitir a los enrutadores (*routers*) reenviar el tráfico basándose, no en la dirección de destino, como ocurre en el tradicional enrutamiento IP, sino en una "etiqueta" insertada en la cabecera del paquete. Analizando esta etiqueta, el *router* determinará así cual es el próximo salto o "*next-hop*" para el paquete. Este procedimiento hace que el proceso de reenvío quede desligado del protocolo de enrutamiento en sí, lo cual nos lleva a la propia definición de "Multiprotocolo", de MPLS, que viene impulsada del hecho de que puede funcionar sobre diversos protocolos como Ethernet, FR, ATM o IP.

El protocolo MPLS viene descrito como muchos otros protocolos desarrollados por el IETF en una RFC (*Request For Comments*), en este caso concreto la RFC 3031. [Ref. 1]

2.2 Beneficios de MPLS como tecnología de Backbone/Núcleo

Entre las muchas razones para usar esta tecnología MPLS para el Núcleo de nuestra red de proveedor de servicios, cabe destacar los siguientes aspectos, que sin ser los únicos, si son de los más importantes, cuando queremos resaltar los beneficios de MPLS:

- **Mejora del rendimiento en el proceso de conmutación**: Quizá sea de los beneficios menos destacables a día de hoy, debido al incremento en las capacidades de cómputo de los actuales dispositivos de red, y al hardware dedicado que hoy en día se utiliza (ASIC - *Application-Specific Integrated Circuits*), pero sigue siendo digno de mencionar, ya que en su momento fue un valor añadido de esta tecnología, muy a tener en cuenta. Dicho esto, diremos que en este punto se quiere reseñar que, al contrario que con el enrutamiento IP en el que el *router* había de procesar el paquete hasta la capa 3 del modelo OSI (capa de Red) y realizar una búsqueda para encontrar la coincidencia más larga entre la IP de destino y las entradas de la tabla de rutas; en MPLS utilizamos una tabla de etiquetas que procura un proceso de búsqueda más simple y rápido. Esta tabla de etiquetas, de la cual hablaremos más ampliamente en subsiguientes apartados, nos proporciona información de reenvío asociada con una

coincidencia exacta, lo que permite tablas de reenvío menores y más eficientes que una tabla de rutas IP.

- **Uso de Ingeniería de Tráfico**: Los protocolos de enrutamiento no son capaces de usar todos los recursos de red, debido al simple hecho de que su mecanismo de elección del mejor camino es limitado. El propio protocolo no otorga visibilidad alguna de los recursos que en la red se están utilizando. Es por esto que los *routers* no reconocen cuándo hay enlaces infrautilizados o dónde existe congestión en la red. Por ello, muchos de los enlaces de red sufren lo que se denomina híper-agregación. En este sentido podemos decir que la mayor ventaja de MPLS es la forma en que el tráfico se reenvía a través de la red, puesto que podemos influir en la dirección en la que viajarán los paquetes por la red dotándola de mayor flexibilidad y capacidades. Por ejemplo, evitando ciertos enlaces, usando enlaces con un mínimo de ancho de banda disponible o inclusive, definiendo caminos explícitos para el tráfico, apoyándonos en protocolos como RSVP-TE.

  La ingeniería de tráfico podríamos definirla por tanto como la habilidad que disponemos para llevar a cabo un uso optimizado de los recursos de la red, usando sus dispositivos y enlaces de la forma más eficiente posible.

- **Redes de alta disponibilidad**: Siempre que se presenten fallos en los recursos dentro de la red, ya sea en los dispositivos o en los enlaces que conectan unos a otros, cobra gran importancia la forma en la que la red responde ante ellos, sobre todo, cómo de rápido se reencamina el tráfico hacia otros enlaces carentes de fallos o hacia otros nodos no afectados por problemas. A este lapso de tiempo se le conoce como tiempo de convergencia de la red, y puede ser un punto crítico en entornos de proveedor de servicios como el que nos disponemos a diseñar.

  Los tiempos de convergencia en redes IP sin MPLS pueden tornarse inaceptables para ciertos tipos de tráfico, o inclusive para ciertos tipos de clientes. MPLS brinda la oportunidad de configurar de forma sencilla ciertas características que proporcionan un notable aumento del rendimiento en los tiempos de re-encaminamiento, disminuyendo así el tiempo necesario para conmutar el tráfico de un camino afectado por una falla a otro libre de inconvenientes hacia el destino.

  El uso de la característica *Fast Reroute* o de LSPs (*Label Switched Paths*) secundarios, bien sea en conjunto o de forma independiente, para un camino primario (principal), nos ayudarán a mejorar, esto es disminuir, los tiempo de convergencia de nuestra red IP/MPLS.

  Como se mencionó anteriormente, éste y otros aspectos específicos de nuestra red serán cubiertos en subsiguientes capítulos de manera más detallada.

- **Establecimiento y consolidación de servicios sobre una infraestructura común**: MPLS es una tecnología que habiendo alcanzado un alto grado de madurez en la

redes de operadores, aún hoy sigue evolucionando gracias a su gran versatilidad y a una de sus características de base: el soporte de servicios, aplicaciones y soluciones sobre una infraestructura de red convergente.

2.3 Principales Servicios y aplicaciones disponibles mediante redes MPLS

Hoy en día, con el desarrollo de nuevos y diferentes servicios y en función de su propósito, se hace más importante si cabe la diferenciación y el tratamiento de los diversos tipos tráfico, así como por supuesto, la separación de los diferentes clientes y emplazamientos.

Como ejemplo más plausible, e infinidad de veces usado, tenemos el caso del tráfico de VoIP el cual demanda unas características de bajo retardo (*delay*) y baja variación del mismo (*jitter*) en detrimento de pérdidas esporádicas de paquetes. Algo completamente contrario ocurre con el envío de tráfico de comunicaciones. Ejemplo de ello puede ser el envío de un e-mail, el cual demanda mínima perdida de paquetes, necesarios para componer el mensaje final, pero que, por el contrario, no es crítico en cuanto al retardo que puedan sufrir dichos paquetes en su tránsito de origen a destino.

El aislamiento y seguridad en las conexiones entre emplazamientos de cliente, pasa a día de hoy por la creación de las denominadas Redes Privadas Virtuales (*VPN - Virtual Private Networks*). La creación de una red IP/MPLS de un proveedor de servicios de Internet (ISP), como la que en este proyecto se procede a diseñar, permite la posibilidad de crear, entre otros, servicios VPN corporativos que se encuentran entre las aplicaciones más importantes actualmente siendo una fuente muy significativa de ingresos para los ISPs.

2.3.1 *Virtual Private Wire Service* (VPWS) Servicio VPN punto a punto (Capa 2)

Este es un servicio destinado a clientes que requieran de una conectividad punto a punto dedicada, para conectar dos de sus emplazamientos. En ocasiones podemos encontrar otras denominaciones para dicho servicio, como por ejemplo tubería (*Pipe*) o *Virtual*

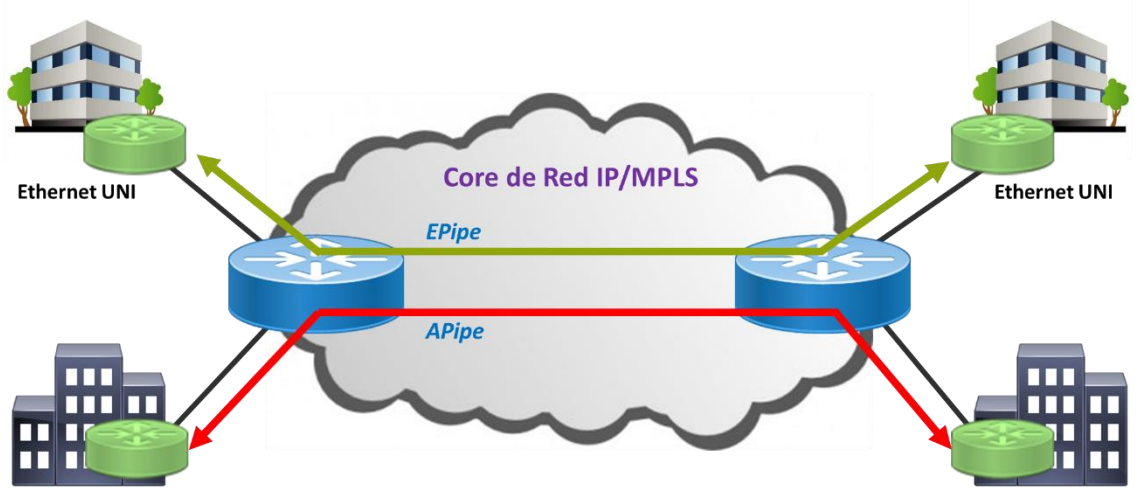


Figura 1: Esquema de Servicios VPWS

Leased Line (VLL), que como su nombre indica, trata de emular una línea privada arrendada sobre la infraestructura global basada en paquetes. Es por ello que, desde una perspectiva de cliente, este servicio VPN (el más simple que podemos encontrarnos, en cuanto a consumo de recursos y simplicidad en su despliegue), actúa como un cable extremo a extremo entre ambas localizaciones de cliente.

Si en ambos extremos la interfaz de acceso a la red (UNI - *User Network Interface*) está basada en tecnología Ethernet, se denominará ePipe (*Ethernet Pipe*).

Este servicio de VPN no está limitado a tecnología Ethernet, sino que MPLS otorga la ventaja de trabajar con tecnologías heredadas como ATM (*Asynchronous Transfer Mode*), FR (*Frame Relay*) o TDM (*Time Division Multiplexing*), gracias a la naturaleza transparente de las conexiones VLL. En estos casos el nombre de la tubería cambiará, encontrando así aPipes, fPipes, cPipes respectivamente, según la tecnología utilizada en el acceso.

2.3.2 *Virtual Private LAN Service* (VPLS) Servicio VPN Multipunto (Capa 2)

Otro de los servicios VPN de capa 2 (referenciando así al modelo OSI), es el servicio VPLS, el cual nos permite crear una conectividad multipunto, entre las diversas sedes de cliente. Si volvemos a usar analogías, este servicio sería el equivalente, bajo la perspectiva de cliente, a un conmutador Ethernet (*Switch*), que conecta varios emplazamientos dispersos geográficamente. Dicha VPLS hace que todas las oficinas (emplazamientos) de cliente pertenezcan al mismo dominio de difusión (*broadcast)*.

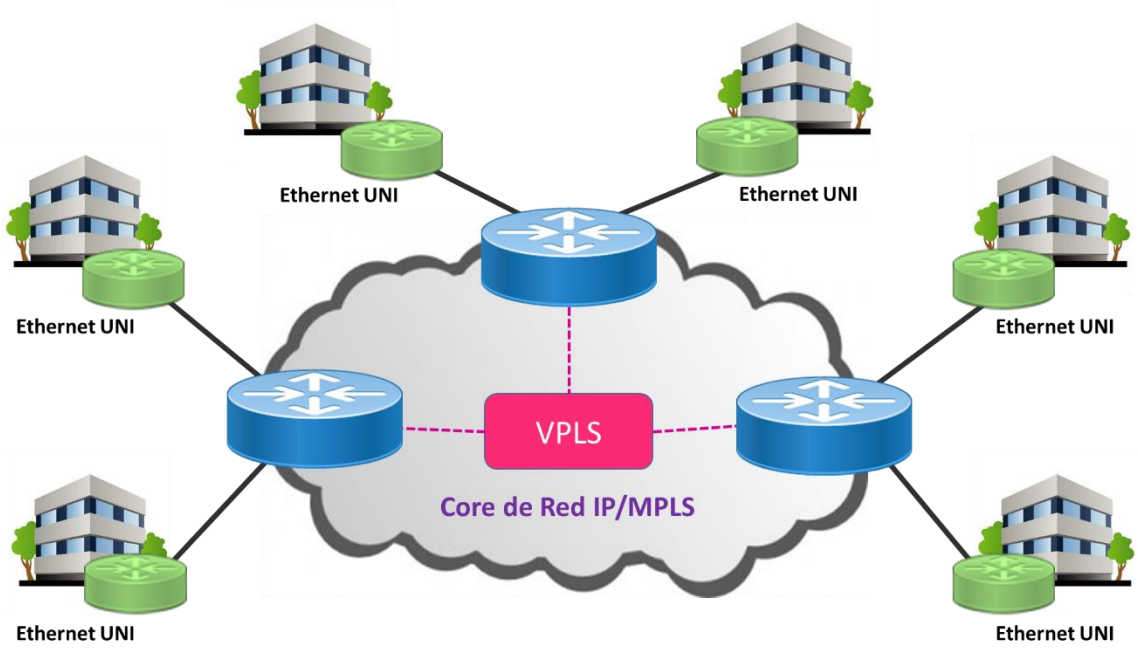


Figura 2: Esquema de un Servicio VPLS

Debido a que es un servicio VPN de capa 2, el proveedor de servicios sólo es responsable de la entrega de conectividad en capa de enlace de datos (basándose en direcciones físicas, esto es, direcciones MAC), recayendo en el cliente la gestión y control del enrutamiento.

Este servicio admite características adicionales, como doble etiquetamiento (*double tagging* también conocido como QinQ), VLAN *trunking* o STP (*Spanning Tree* Protocol), para evitar tormentas de *broadcast*.

2.3.3 *Virtual Private Routed Network* (VPRN) Servicio VPN Multipunto (Capa 3)

Además del mencionado servicio VPLS para conectividad multipunto, existe otro servicio en modalidad multipunto denominado VPRN, nombrado así en los entornos de Alcatel-Lucent como el que nos ocupa. Sin embargo VPRN es un servicio de capa 3. Esto hace

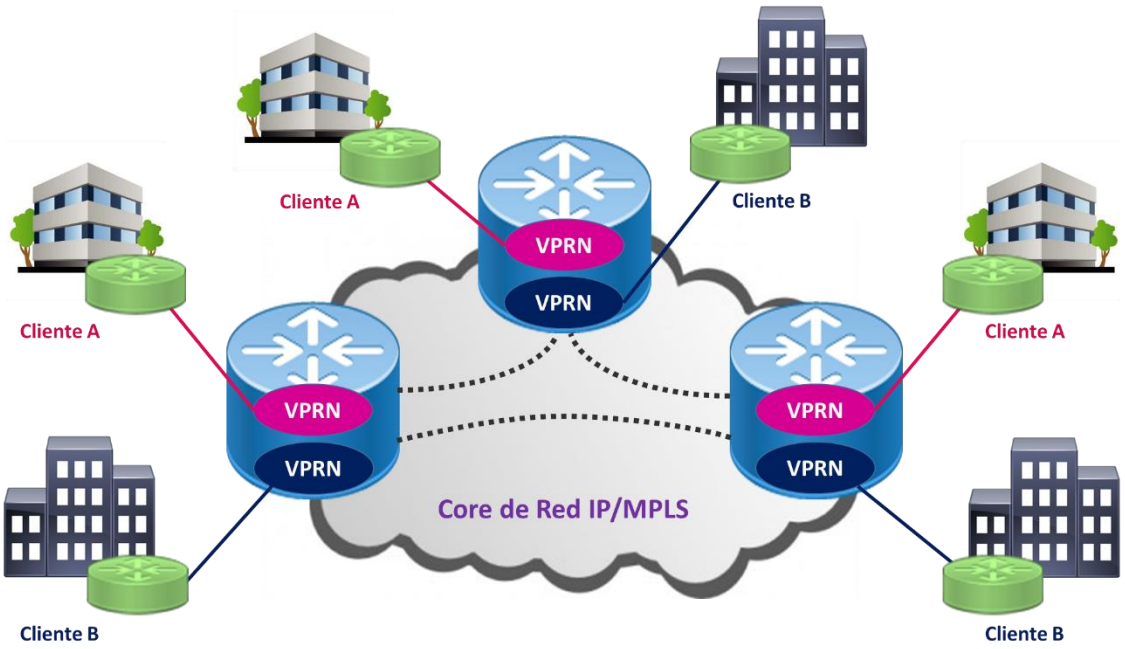


Figura 3: Esquema de un Servicio VPRN

que la gestión del enrutamiento ahora caiga de lado del proveedor de servicios de internet, es decir, en nuestro Núcleo de red a desarrollar. En ocasiones podemos encontrar el término "*peering model*" para tales soluciones, ya que ha de existir una relación de "emparejamiento" (*peering*) o interconexión entre los equipos de acceso de cliente (CE - *Customer Edge*) y los del frontera del *core* de red (PE - *Provider Edge*).

Las principales preocupaciones que puede haber acerca del aislamiento de los cliente en los entornos VPN-IP, se solventan en este servicio a través de unas instancias denominadas VRF (*Virtual Routing and Forwarding*). A cada cliente se le asigna una VRF, que a fin de cuentas, representa una instancia de enrutamiento distinta ("*router* virtual propio"). Por tanto, nos permite un aislamiento de la información de enrutamiento por

cliente y, como consecuencia, la posibilidad de solape de direccionamiento privado (*ovelapping*). Esto es, los clientes pueden utilizar el mismo espacio de direcciones IP privadas, sin temor a que éstas se solapen con las usadas por otros clientes.

El aislamiento entre clientes se logra de manera inherente en el Núcleo, gracias al uso de túneles, que emplean etiquetas únicas para cada servicio. Hablaremos un poco más en profundidad de este servicio cuando definamos qué son y para qué se usan los túneles de servicio, así como de los protocolos para la distribución de las etiquetas de servicio que hacen posible la creación de estos túneles. (Véase apartado 2.6.9.2)

2.4 Visión general de MPLS

2.4.1 Resumen del enrutamiento tradicional basado en IP

Antes de comenzar con la introducción a MPLS, es necesario prestar una visión general del enrutamiento tradicional que se ha venido utilizando en las redes IP, para así ser capaces de entender en mayor medida las ventajas que nos brinda el encaminamiento basado en etiquetas de MPLS.

El proceso de reenvío de paquetes IP extremo a extremo en redes IP se ha confiado siempre al modelo de funcionamiento *hop-by-hop*, salto a salto. Así, la decisión de reenvío se lleva a cabo independientemente en cada equipo de enrutamiento que recibe el paquete en la red, y que conforma un salto dentro del camino global que seguirá el paquete.

Todos los enrutadores (*routers*) de la red, construyen su propia tabla de rutas usando para ello rutas estáticas o protocolos de enrutamiento dinámico, y la información que reciben de otros enrutadores.

El mecanismo general es el siguiente: Cuando el paquete de información (paquete IP) llega al router, éste usa su tabla de rutas para determinar el siguiente salto en el camino del paquete, basándose en un algoritmo de mayor coincidencia (*Longest Prefix Match*). La tabla de rutas posee una lista de redes de destino con las direcciones de los siguientes saltos correspondientes para alcanzarlas.

Si desglosamos los pasos a seguir serían los siguientes:

1. Revisión y posterior eliminación de la cabecera de capa 2, que encapsula el paquete IP.
2. Posteriormente se examina la cabecera de capa 3 (IP), y se lleva a cabo una búsqueda, usando la dirección IP de destino, basada en la coincidencia más larga, dentro de la tabla de enrutamiento.
3. Una vez se encuentra la coincidencia más larga entre la dirección de destino IP y una de las entradas de la tabla de enrutamiento, se determina la interfaz del siguiente salto asociada.
4. Se construye la cabecera de capa 2 para el encapsulamiento del paquete IP, correspondiente a la interfaz de salida hacia el próximo enrutador (siguiente salto).

Resumiendo, cuando se recibe un paquete, cada *router* decide el mejor camino sobre el que reenviar el paquete, usando la tabla de enrutamiento de capa 3 y sus asociaciones de capa 2.

2.4.2 Nomenclatura y Terminología en escenarios IP/MPLS

Antes de comenzar a utilizar términos relacionados con el protocolo MPLS hemos de familiarizarnos con la nomenclatura y terminología asociada. Es por ello que aquí se recogerán los elementos más importantes que componen las redes IP/MPLS y algunas entidades lógicas que nos ayudan a comprender el funcionamiento del protocolo. La siguiente figura ofrece una visión general del emplazamiento de cada una de las entidades que se definirán a continuación.

Figura 4: Entidades funcionales en una Arquitectura MPLS

- ***Label Edge Router (LER):*** Como su nombre indica, son equipos de frontera, entre el dominio MPLS y el dominio de cliente, similar al concepto del PE solo que este nombre hace referencia a la función que desempeña el propio router dentro del proceso de reenvío en MPLS. Un LER puede ser:
  - **Ingress LER (iLER):** Es el punto de entrada del tráfico que no es MPLS. El iLER añade las etiquetas al tráfico (no MPLS) entrante y lo envía al siguiente salto, un LSR.
  - **Egress LER (eLER):** El tráfico MPLS sale de la red MPLS a través de estas entidades. El eLER elimina las etiquetas de los paquetes MPLS y envía dichos paquetes (ya sin etiqueta) hacia los routers de cliente (CE).
- ***Label Switched Router (LSR):*** El principal propósito de un LSR es recibir el tráfico etiquetado y reemplazar la etiqueta en entrada por la correspondiente en salida antes de reenviar el tráfico hacia el enrutador del próximo salto. De este modo, el concepto LSR es un concepto más general que el de LER.

  La distinción de un enrutador dentro de la categoría de iLER, eLER o LSR sólo depende de en dónde esté emplazado el router, de la dirección del flujo del tráfico y del origen y destino (CE-CE). Un flujo de tráfico con idénticos extremos

puede definir distintos roles en los enrutadores, dependiendo de la dirección. Véase la figura 4.

- ***Label Switched Path (LSP):*** Puede describirse como el camino que conecta dos Label Edge Routers dentro de una red MPLS, y que queda definido por la secuencia de etiquetas y las acciones de reenvío realizadas por los encaminadores para transportar los paquetes de un punto a otro de la red usando la conmutación de etiquetas. Un LSP tiene siempre como punto de partida un iLER y como punto final un eLER. Por consiguiente, un LSP es un camino unidireccional y extremo a extremo. Al ser unidireccional, el LSP definido para transportar el tráfico de un "Router A" hasta un "Router B", puede no coincidir en su recorrido con el definido para llevar el tráfico de regreso, del "Router B" al "Router A". La encapsulación y el reenvío de paquetes usando etiquetas a veces es denominado "*tunneling*"; de esta forma, los LSP's a menudo son referidos como túneles.

  Dichos túneles han de establecerse previamente al envío de los paquetes de información. La negociación y distribución de etiquetas a cargo de algunos protocolos como LDP o RSVP-TE para establecer los túneles se discutirá en detalle más adelante.
- ***Forwarding Equivalence Class (FEC):*** Esencialmente este concepto hace referencia al grupo de paquetes que son enviados de la misma manera, con el mismo tratamiento y siguiendo el mismo camino. Esto posibilita la clasificación de los paquetes en grupos basándonos en un criterio común. En las tradicionales redes IP, el FEC normalmente corresponde al prefijo de la tabla de rutas que coincide con el destino del paquete. De esta forma, en dichas redes, la clasificación del paquete en un FEC se realiza a cada salto.

  Por definición el FEC puede basarse en cualquier criterio administrativo, como el marcado que lleva el paquete indicando la Clase de Servicio, o incluso, la propia dirección origen del paquete.

  En una arquitectura IP/MPLS, pueden usarse diversos criterios administrativos, como los mencionados anteriormente. Además, la clasificación para determinar a qué FEC pertenece el paquete entrante se lleva a cabo una sola vez a la entrada de la red en el router de ingreso (iLER), determinando así cual será la etiqueta que llevará el paquete, y por tanto el túnel que utilizará del origen al destino. Véase figura 5.

  Los túneles (LSPs) se establecen antes del envío de los paquetes de información, antes de que éstos alcancen el primer router de ingreso (iLER). Cuando ya se conoce la etiqueta asociada a cada túnel, el iLER decidirá si el paquete de información que llegue, se reenviará mediante un enrutamiento IP (basado en la dirección destino del paquete), o mediante conmutación de etiquetas. Esta elección vendrá dada por la configuración del servicio del router asociado en la interfaz de entrada por la cual se recibe el paquete.

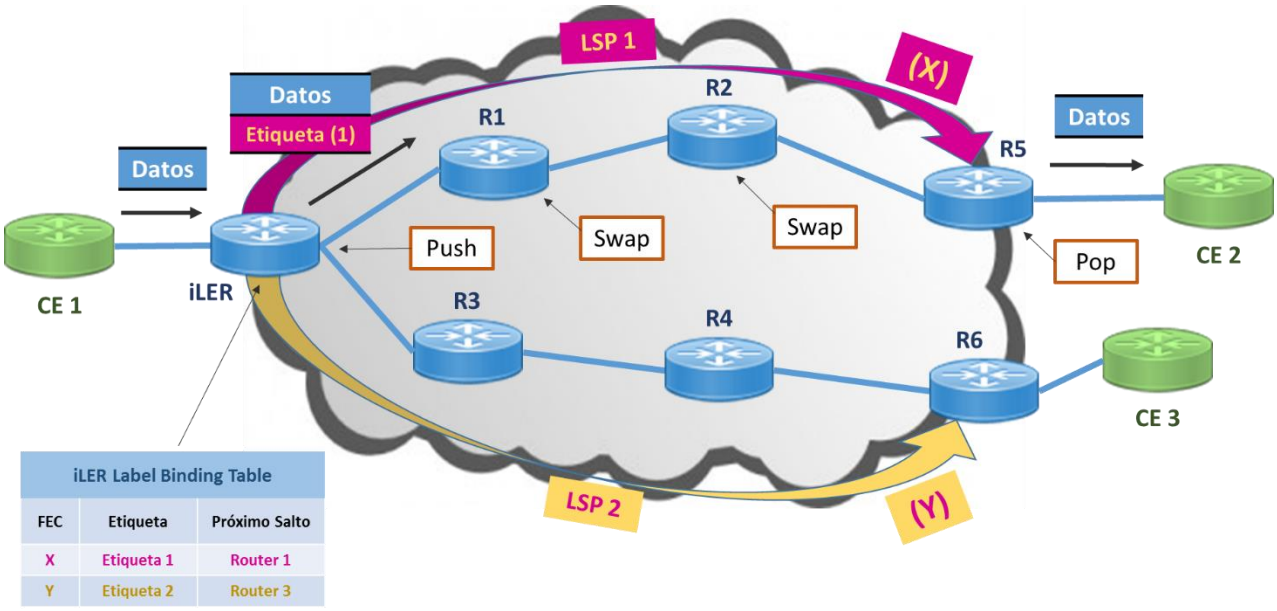


Figura 5: Búsqueda de Información de Reenvío por Etiquetas en el Ingreso

Si el router decide usar la conmutación de etiquetas, el iLER elegirá el túnel a utilizar y etiquetará (insertará la etiqueta) en el paquete antes de reenviarlo hacia el siguiente LSR. Los diferentes LSR's a lo largo del camino entre el iLER y el eLER, no tienen necesidad de reclasificar el tráfico, sino que únicamente, conmutarán las etiquetas de entrada por las correspondientes etiquetas de salida, negociadas anteriormente en la fase de establecimiento de los túneles (que puede ser manual o dinámica mediante protocolos de distribución de etiquetas).

- ***Provider Edge Router (PE):*** Son equipos localizados en la "frontera" del Núcleo de red del ISP. De este modo, poseen al menos una interfaz que está directamente conectada con los CEs de cliente, y al menos una interfaz que se conecta a dispositivos del *backbone* del proveedor de servicios (P *routers*). Es por esto que los PEs deben ser capaces de conectarse a diversos dispositivos CE de cliente y sobre diversos medios de acceso. Los PEs podrían verse desde la perspectiva de cliente como "*gateways*" (puertas de salida) hacia los servicios de VPN que nos brinda el proveedor de servicios. Son equipos versátiles, de alto rendimiento y desempeño, con soporte para un gran número y variedad de interfaces.
- ***Provider (Backbone/Core) Router (P):*** Son el equipamiento de *Backbone* o *Core* (*Routers* localizados en el núcleo de la red del ISP). Nunca se conectan directamente a los equipos de cliente y son los responsables de proporcionar el ancho de banda requerido por el proveedor de servicios y sus requerimientos de conmutación. Como veremos más adelante, se centran en mover un elevado volumen de tráfico a la mayor brevedad posible,
- ***Customer Edge Router (CE):*** Residen en domicilio de cliente. Son los responsables de ofrecer conectividad a las dependencias de cliente facilitando el acceso a la red del ISP por medio de enlaces hacia uno o más equipos de frontera

(PEs). Típicamente el cliente suele ser el dueño y gestor (operador) de estos equipos, pero en ocasiones existen contratos, sobre todo en modalidades de acceso para corporaciones, en los que el propio ISP se hace cargo de la puesta en marcha, mantenimiento y actualización o reemplazo de dicho equipamiento, así como de su gestión. Cabe destacar que estos equipos no poseen constancia de los protocolos de "*tunneling*" o inclusive de los servicios VPN que se proporcionan por parte del ISP.

2.4.3 Proceso de conmutación de etiquetas: *Push, Swap & Pop*

En este punto vamos a ilustrar el proceso de conmutación que tiene lugar dentro del denominado "plano de reenvió".

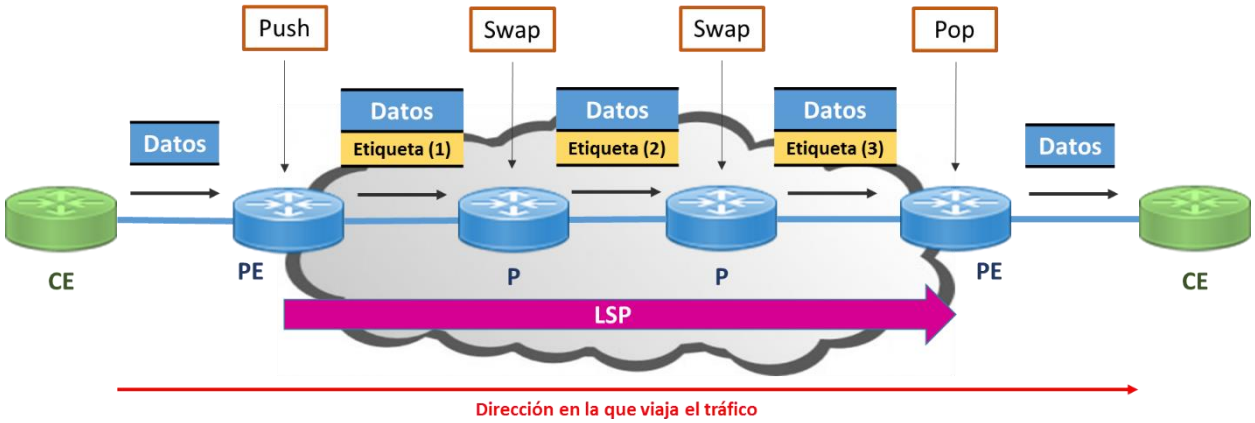


Figura 6: Operaciones Push, Swap & Pop

Una etiqueta (*label*) es un identificador adicional, de longitud fija, que se inserta a la entrada de una red MPLS, en nuestro caso, del núcleo de red del proveedor de servicios. Este proceso de inserción ocurre dentro del primer PE de entrada a la red, que se encuentra unido al CE de cliente. A esta operación de inserción de etiqueta recibe el nombre de "*Push operation*".

El paquete procedente del router de cliente (CE) puede ser de cualquier clase de tráfico no-MPLS, dependiendo del tipo de servicio.

Los routers P simplemente comprobarán la etiqueta que trae el paquete y buscarán una coincidencia con la información de su *Label Forwarding Information* Base (LFIB), o tabla de información para el reenvío por etiquetas, con el fin de encontrar la interfaz de salida para el paquete y la etiqueta necesaria que debe llevar en salida. A este intercambio de etiquetas, entre entrada y salida, para el mismo paquete, es a lo que denominamos operación "*Swap*".

Una vez alcanzamos el router PE al otro extremo del camino o LSP, éste elimina la etiqueta con la que llega el paquete, operación conocida como "*Pop*", y lo reenviará, ya desetiquetado (es decir, sin etiqueta alguna), hacia el router cliente (CE) de destino correspondiente.

La estructura de la etiqueta en sí, así como el apilado de etiquetas, que puede llevarse a cabo con esta tecnología, se explicará más adelante en otro punto del proyecto.

2.4.4 Conceptos: Plano de Control y Plano de Datos (o Reenvío)

Hoy en día cualquier enrutador que se precie y que esté destinado al reenvío de grandes cantidades de información dentro de una red de operador de servicios, posee una distinción entre lo que denominamos Plano de Control y Plano de Datos.

El procesado de los paquetes de información y su reenvío tiene lugar en el Plano de Datos, y lo que denominaríamos "centro de mando" o "inteligencia" correría a cargo del Plano de Control, el cual se encarga de la interacción con otros routers a través de protocolos y de las principales funciones de mantenimiento. Es por esta razón por la que el Plano de Control ha de definir con antelación cómo ha de comportarse el enrutador, antes incluso de que la información llegue hasta sus interfaces.

Esta división de funciones corresponde con una división en los componentes de hardware dentro del sistema. Así, en los enrutadores de Alcatel-Lucent SR que utilizaremos en nuestro despliegue de la implementación de la red de operador, la parte de hardware que realiza las funciones del Plano de Control se denomina "*Control Processor Module*" o CPM, y el hardware destinado para llevar a cabo las labores del Plan de Datos y por tanto a procesar y reenviar los paquetes corre a cargo de las tarjetas "*Input Output Modules*" o IOMs.

2.4.4.1 Plano de Control y Plano de Datos en IP:

Cuando un protocolo de enrutamiento se habilita en un *router*, se llevan a cabo una serie de funciones. Con los actuales protocolos de encaminamiento ("*routing*") como OSPF (*Open Shortest Path First*) e IS-IS *(Intermediate System – Intermediate System*), se establecen relaciones de adyacencia entre ellos. Si ambos routers están de acuerdo en

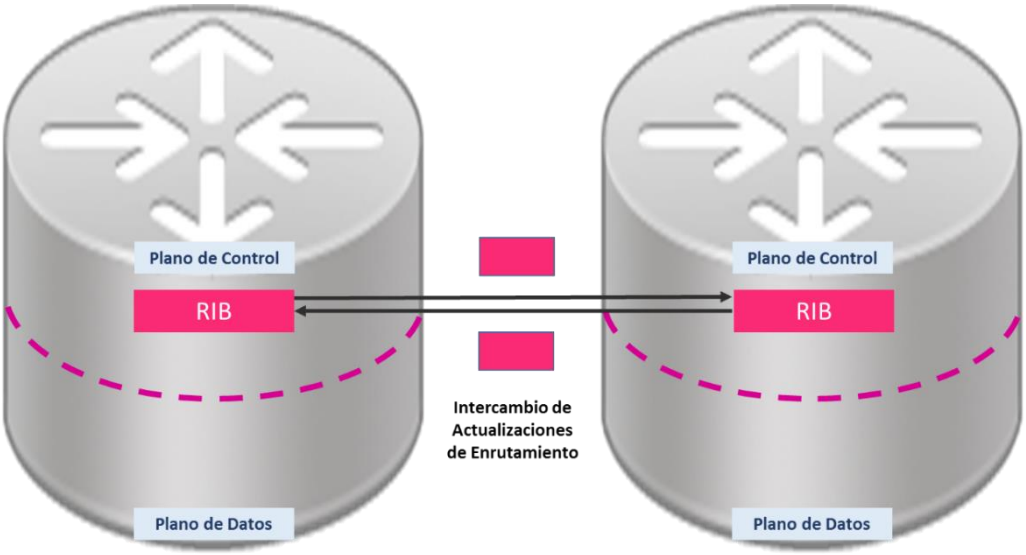


Figura 7: Plano de Control IP y el intercambio de Actualizaciones de Enrutamiento

los parámetros de su asociación, intercambiarán actualizaciones de enrutamiento entre sí para sincronizar sus bases de datos topológicas y poder así construir la *Routing Information Base* (RIB), base de datos de información de enrutamiento.

Durante el desarrollo de este proyecto sólo se considerarán los protocolos de estado de enlace, ya que son los más ampliamente utilizados en los entornos de proveedor de servicios como es el caso que nos ocupa.

Dentro de la RIB, podemos encontrarnos con varias alternativas como próximo salto para destinos específicos. Es responsabilidad del enrutador decidir y escoger los mejores caminos de entre todos los posibles para los destinos dados. En el caso de los protocolos de estado de enlace, esta decisión se basa en la ejecución del algoritmo SPF (*Shortest Path First*) derivado de algoritmo de Dijkstra.

El algoritmo SPF usa las métricas del protocolo elegido para calcular el mejor camino. En estos protocolos de estado de enlace la métrica se define en función del ancho de banda del enlace. Cuanto mayor es el ancho de banda, menor es la métrica para dicho enlace, y por tanto disminuye el coste de alcanzar el destino mediante ese enlace.

Una vez calculados los costes, el enrutador (CPM) coloca la interfaz elegida, que me llevará al destino mediante menor coste, en la Tabla de Rutas. Esta información pasará entonces al Plano de Datos para que ésta pueda usarse en las funciones de reenvío. La base de datos donde se alojará esta información es la llamada FIB (*Forwarding Information Base*). En los Alcatel-Lucent SR existirá una copia idéntica de la FIB en todas las tarjetas IOM que se encuentren operativas.

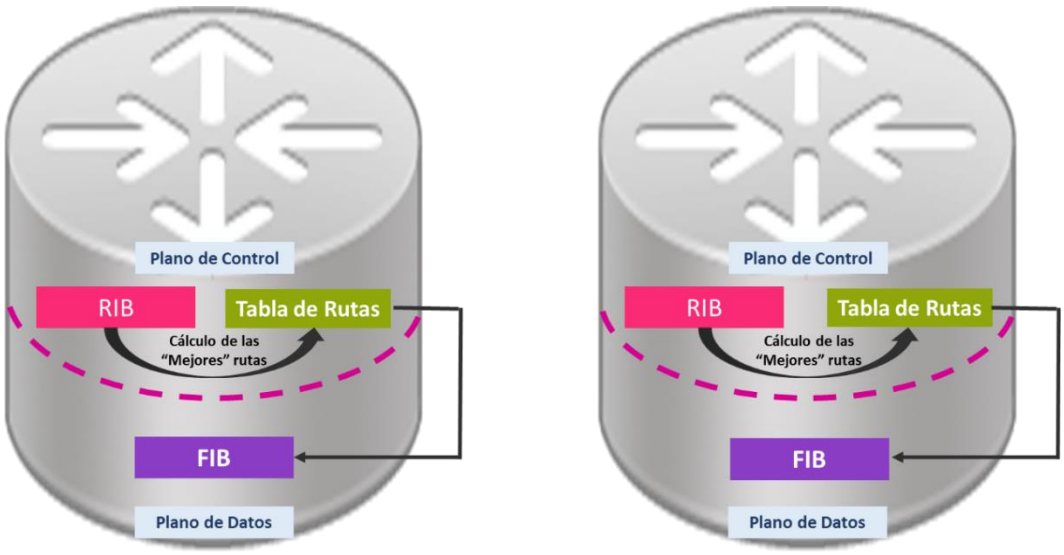


Figura 8: Plano de Control IP y su interacción con el Plano de Datos

Para mantener las FIBs actualizadas y sincronizadas, existen procesos internos dentro del propio enrutador. Una vez tenemos la FIB establecida, el *router* la usará para el reenvío de paquetes de tráfico IP nativo (sin etiquetar).

2.4.4.2 Plano de Control y Plano de Datos en MPLS:

Para establecer un núcleo de red con capacidades MPLS es requisito indispensable la configuración de un IGP (*Interior Gateway Protocol*) ya que, cuando se inicia un protocolo de señalización de etiquetas en MPLS, los routers han de establecer sesiones previamente, y es la información presente en las tablas de rutas la que permite a los enrutadores crear estas sesiones.

Después del establecimiento de estas sesiones, los routers intercambian sus etiquetas, asociadas a los FECs (ej.: prefijos de destino IP) y que son conocidas por ellos (las propias y las recibidas de otros routers). Toda esta información que se envía y se recibe se almacena en la *Label Information Base* o LIB.

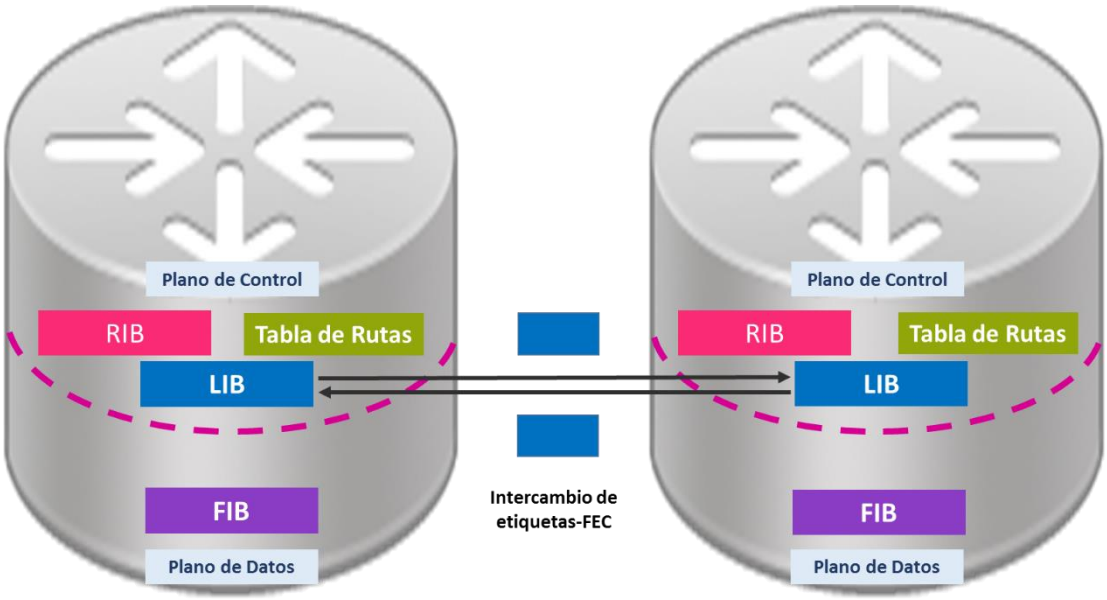


Figura 9: Plano de Control MPLS y el intercambio de uniones etiqueta-FEC

Una vez finaliza este proceso en el camino de extremo a extremo de un LSP (túnel), se puede llevar a cabo el reenvío basado en etiquetas.

Como ocurre con el tráfico IP nativo (sin etiquetas) en el que utilizábamos una FIB, en este caso, la información que se precisa para el reenvío basado en etiquetas dentro del plano de Datos, se almacena en la LFIB (*Label Forwarding Information Base*).

Se ha de ejecutar un proceso de selección dentro de la LIB para la construcción de la LFIB. De este modo, la LIB puede contener entradas redundantes que no se usen en el plano de datos (LFIB). La elección de las etiquetas a usar, y por tanto, de las entradas que contendrá la LFIB, dependerá del protocolo MPLS de distribución de etiquetas que se haya implementado, bien sea LDP (*Label Distribution Protocol*) o RSVP-TE (*Resource Reservation Protocol –Traffic Engineering*).

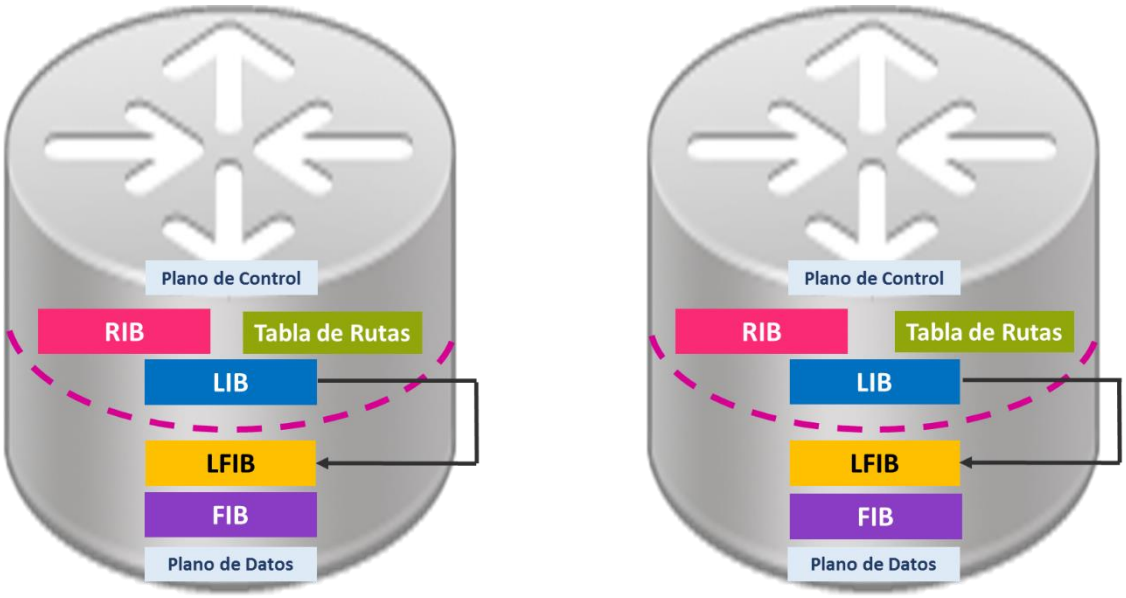


Figura 10: Plano de Control MPLS y su interacción con el Plano de Datos

Detallaremos en profundidad LDP en apartados posteriores de este capítulo.

Cuando se recibe un paquete en el iLER, éste toma la decisión de sobre qué túnel MPLS (LSP) reenviará el tráfico. Cómo ya se mencionó anteriormente, esto dependerá de la definición del servicio con el que esté asociado la interfaz.

En el caso en el que el iLER decida usar un túnel MPLS para reenviar los paquetes, habrá de realizar una búsqueda en su tabla LFIB basada en el FEC. Este proceso dotará a los paquetes con la etiqueta seleccionada, y serán enviados al correspondiente próximo LSR.

Para simplificar el caso, se ilustra el concepto con la conmutación de una única etiqueta. Sin embargo, en realidad, más de una etiqueta se añade normalmente al tráfico de datos, dependiendo del tipo de servicio o aplicación en cuestión. Esto es lo que denominamos apilamiento de etiquetas, que se explicará más adelante.

El LSR entonces intercambiará la etiqueta por otra, de nuevo, consultando la LFIB almacenada localmente en su plano de Reenvío. Excepcionalmente un LSR puede añadir una etiqueta adicional a la pila, en entrada, además de llevar a cabo el proceso de intercambio de etiquetas. Esto se detallará posteriormente.

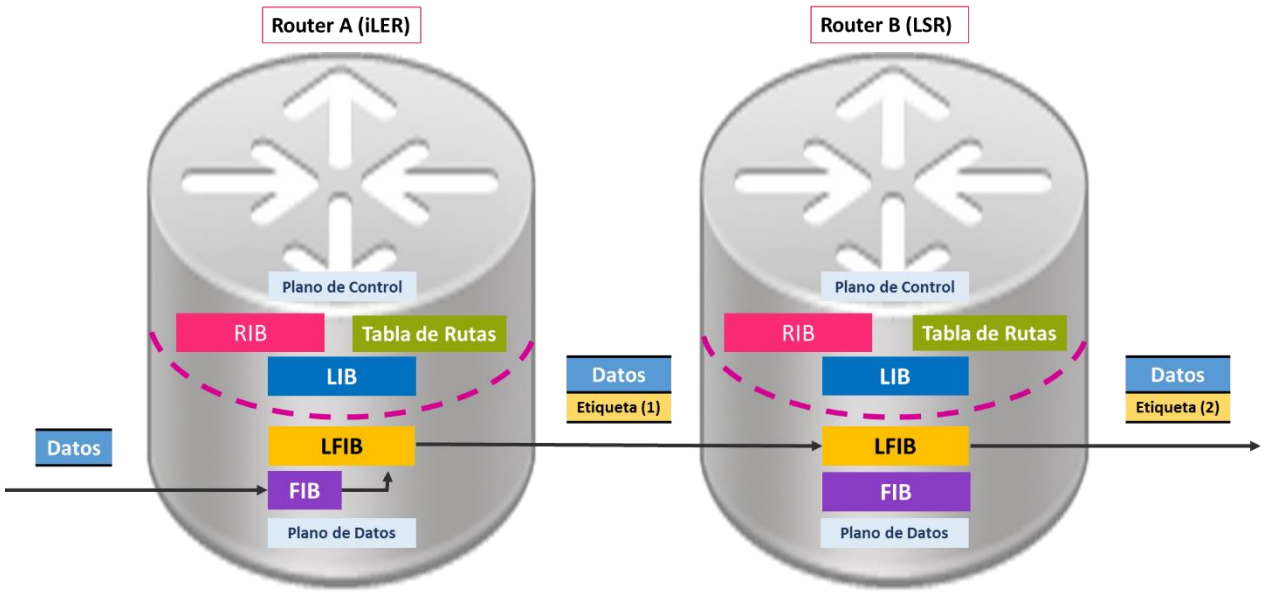


Figura 11: Ejemplo de reenvío información en MPLS – iLER & LSR

Finalmente, el eLER que reciba el tráfico será el *router* de último salto en MPLS, en el cual acaba el túnel. Dicho enrutador eliminará la etiqueta(s) del paquete entrante, buscará la interfaz de salida, y finalmente reenviará el paquete de información original fuera del *backbone*/núcleo MPLS hacia el CE destino.

2.5 Fundamentos de MPLS

En este punto introduciremos los conceptos relacionados con el reenvío de paquetes en el plano de Datos, el apilamiento de etiquetas en MPLS, su aplicación en los servicios VPN, y los campos de la cabecera de la etiqueta MPLS.

En una segunda parte de este mismo apartado hablaremos acerca de los principios generales del plano de Control en los protocolos de señalización dinámicos de MPLS. Veremos, desde una perspectiva genérica la distribución de etiquetas y los modos de control y retención. La verdadera operativa de estos modos depende del protocolo implementado, que será cubierto más tarde en la operativa y funcionamiento del protocolo LDP.

2.5.1 Pila de etiquetas en MPLS

Las etiquetas de MPLS se insertan entre la capa 2 de la interfaz de red y la carga útil que encapsula MPLS. Como ya se mencionó anteriormente, inicialmente MPLS transportaba paquetes IP a sus FEC destino gracias a la encapsulación con etiquetas, proporcionando mayores rendimientos en la red. Por esto, MPLS a veces es conocido como un protocolo

de capa 2.5, debido a que la etiqueta se inserta entre las cabeceras de capa 2 y de capa 3.

Hoy en día MPLS también soporta servicios VPN, así como túneles IGP y BGP. Por tanto, la carga útil de MPLS puede consistir en una amplia variedad de protocolos y servicios. Durante el proyecto nos referiremos a la carga útil como "Datos", de una manera general.

Una pila de etiquetas puede formarse por la encapsulación de etiquetas sobre otras etiquetas, cada una de las cuales proporciona una función específica en la red. Ejemplo de ello podría ser la introducción por parte del PE de una etiqueta de servicio en la carga útil con el fin de identificar la VPN a la que pertenece el tráfico. Después, el mismo enrutador añadiría una segunda etiqueta, en la cima de la pila, para mover el paquete etiquetado a través de la red MPLS, como etiqueta de transporte. Si esta red de operador estuviera usando la característica de *Fast Reroute*, el enrutador añadiría además una tercera etiqueta a la pila. Los routers de servicio de Alcatel-Lucent soportan hasta seis etiquetas apiladas. Aunque técnicamente el paquete puede llevar cualquier número de etiquetas, todo depende del tamaño máximo de paquete de la interfaz (MTU – Maximum Transmission Unit).

La necesidad de soportar este tipo de apilamiento es una consecuencia directa del uso compartido de un consistente y robusto *backbone* de red. Las redes IP/MPLS de los proveedores de servicios como la que desplegaremos, han de soportar todos los servicios de cliente, teniendo en cuenta la escalabilidad y las soluciones VPN basadas en estándares.

Los conceptos más importantes que hay que entender aquí son, el concepto de "*tunneling*" y el apilamiento de etiquetas.

Si volvemos al ejemplo anterior, y pensamos en la construcción de un servicio de conectividad punto a punto, sólo los enrutadores de borde (PEs) serían conscientes de los servicios en sí. Por cada VPN de cliente que creamos, las instancias de servicio se configuran en todos los PEs que participen, entendiendo por instancias de servicio esas entidades de software virtuales que proporcionan un aislamiento entre los diferentes clientes. Además de esto, las instancias de servicio sirven para proporcionar seguridad (gracias al aislamiento) y para aplicar modificaciones particulares en los ajustes, dentro de cada servicio de cliente. El uso de estas entidades lógicas hace que pueda llevarse a cabo una asignación más granular y escalable de los recursos de red para los diferentes clientes de manera diferenciada.

Los túneles de servicio, separados lógicamente (diferentes etiquetas de servicio), conectan las instancias de servicio que pertenecen al mismo cliente en los distintos PEs. Mientras que los túneles de transporte MPLS pueden multiplexar y transportar varios túneles de servicio al mismo tiempo. El enrutador intermedio (P) es únicamente consciente del túnel de transporte. Este túnel de transporte esconde (a través del apilamiento de etiquetas) los túneles de servicio a los routers P. Debido a que estos encaminadores intermedios no tienen visibilidad de las instancias de servicio, o de los

túneles de servicio que conectan estas instancias, éstos sólo necesitan mirar la etiqueta exterior para realizar las decisiones de reenvío de tráfico, lo cual ayuda a mejorar el rendimiento y la escalabilidad de la red del proveedor de servicios.

2.5.2 Encapsulación MPLS para servicios VPN de capa 2

Los servicios VPN de capa 2 y capa 3 tratan de forma diferente los paquetes de cliente.

Los principales servicios VPN de capa 2, *Virtual Private Wire Services* (VPWS) y Virtual *Private LAN Services* (VPLS), son transparentes para el cliente, en el sentido de que el servicio reenvía toda la carga útil de capa 2 generada por el cliente transparentemente, de un dispositivo CE a otro CE del mismo cliente.

Si asumimos como capa de enlace Ethernet, en el siguiente ejemplo de la Figura 12, el enrutador CE1 usará como dirección MAC de origen la de CE1 y como destino la de CE2 (1). El router A (encaminador de ingreso) encapsulará la trama completa (2) junto con las dos etiquetas MPLS de transporte y de servicio, y una cabecera para la trama

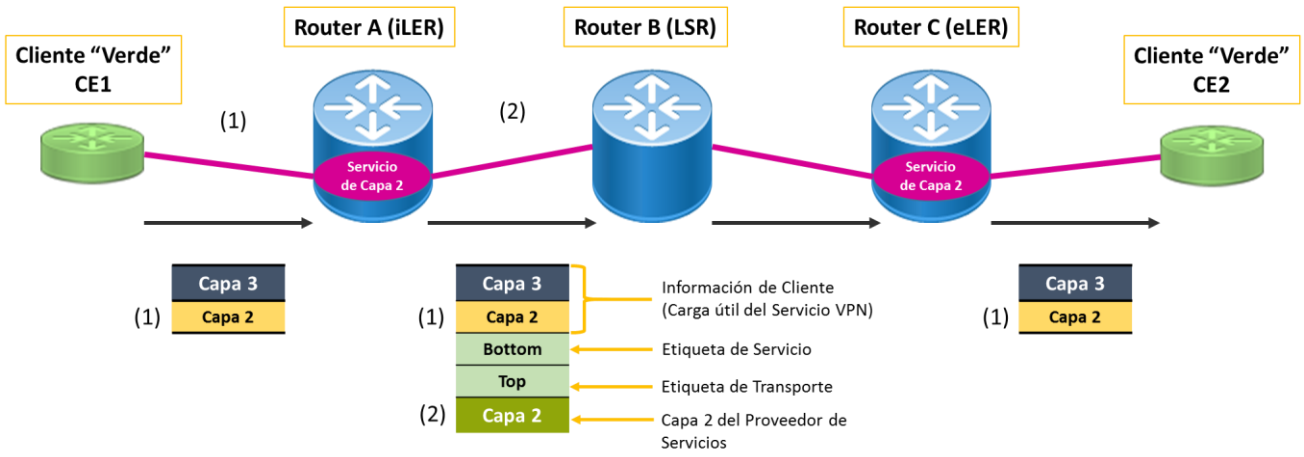


Figura 12: Encapsulación MPLS para servicios VPN de capa 2

Ethernet. Para esta nueva trama, la cabecera plasmará en la dirección MAC de origen la de interfaz de egreso del Router A, y como MAC destino la de ingreso en el Router B (siguiente salto). La etiqueta de transporte, en la cima de la pila (*Top*) será la responsable de "tunelizar" el tráfico del cliente "Verde", desde el ingreso hasta su salida en el LER de egreso (eLER), el Router C. Por su parte, la etiqueta de servicio, en la cola de la pila de etiquetas (*Bottom*), identificará el servicio de borde a borde al que pertenece la carga útil.

2.5.3 Encapsulación MPLS para servicios VPN de capa 3

La solución de servicio VPN de capa 3 es la *Virtual Private Routed Network* (VPRN).

En esta solución, las instancias de servicio mantienen tablas de rutas independientes y aisladas, y se decide en base al propio servicio cómo se reenviarán los paquetes hacia el destino. Los routers PE forman relaciones de emparejamiento con los routers CE de cliente dentro de cada respectiva instancia de servicio.

De nuevo, si asumimos como capa de enlace Ethernet, la cabecera de capa 2 enviada desde CE1 (1) hacia el Router A tendrá como MAC origen la dirección de CE1 y como destino la de la interfaz de servicio del PE (Router A) al que está conectado. De este modo, desde la perspectiva de cliente, el Router A es el siguiente salto hacia la red de destino, CE2.

El Router A o *router* de ingreso, eliminará la cabecera de capa 2, procesará el paquete IP y reenviará sólo la cabecera de capa 3 y la carga útil encapsulándolo junto con las dos etiquetas MPLS (2), y utilizando la cabecera de capa 2 de la interfaz de egreso del proveedor de servicios. La dirección de origen será la de la mencionada interfaz de egreso y como destino aparecerá la dirección MAC del Router B que recibirá la trama.

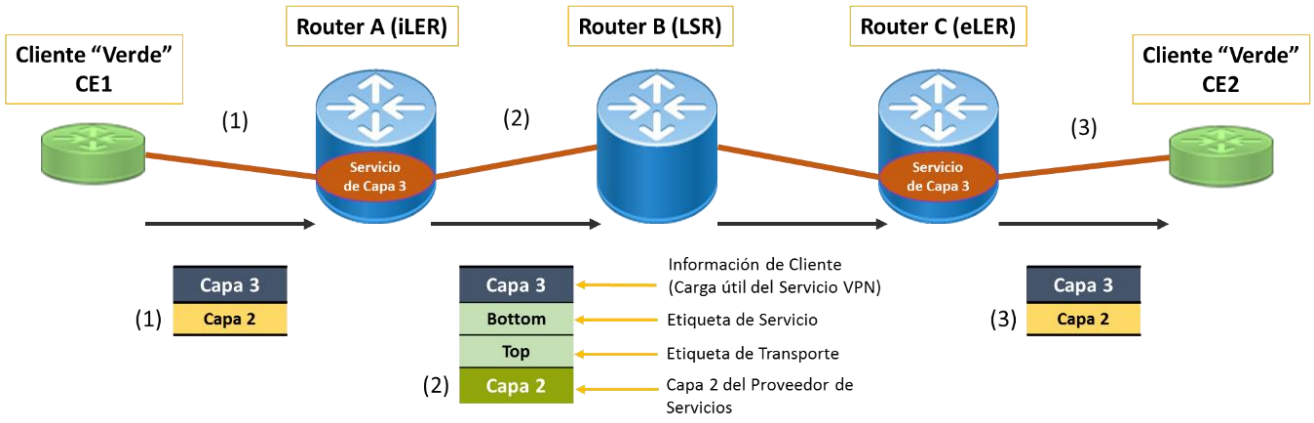


Figura 13: Encapsulación MPLS para servicios VPN de capa 3

Por su parte, cuando le llegué la trama, el Router C (router de egreso o eLER) eliminará las cabeceras usadas en el servicio y procesará el paquete como haría con cualquier otro paquete IP, buscando una ruta para el mismo en la tabla de rutas propia del servicio (VRF). Para el reenvío del paquete (3), el Router C construirá una nueva cabecera de capa 2 usando como MAC origen la dirección de la interfaz de servicio del Router C y como destino la de la interfaz de CE2.

2.5.4 Etiqueta MPLS

Cada etiqueta MPLS en la pila (*stack*) es de tamaño fijo (4 bytes) e incluye los siguientes cuatro campos:

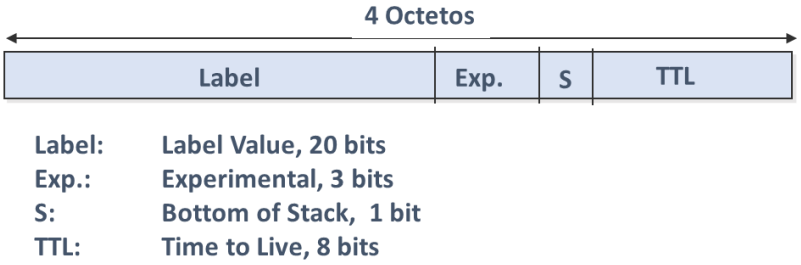


Figura 14: Etiqueta MPLS

Valores para la Etiqueta	Uso de la Etiqueta
0-15	Etiquetas reservadas (Uso especial)
16 – 31	Reservadas para uso futuro
32 – 1023	Reservadas para LSPs estáticos
1024 – 2047	Reservadas para uso futuro
2048 – 18431	Asignadas estáticamente para servicios.
18432 – 32767	Reservadas para uso futuro
32768 – 131071	Asignadas dinámicamente por protocolos MPLS
131072 - 1048575	Reservadas para uso futuro

Tabla 1: Valores posibles para el campo "Label" de la Etiqueta MPLS

- ***Label (20 bits):*** Los 20 bits más significativos de la cabecera MPLS conforman el campo "etiqueta", que contiene la información más importante. Las etiquetas pueden tomar valores dentro de un rango muy amplio (0-1048575). En la Tabla 1 vemos la división del rango en subconjuntos (*pools*) que son usados para diversos propósitos y aplicaciones.
- ***EXP (3 bits):*** Los tres bits siguientes son los denominados bits experimentales. Se les llama así porque en los inicios e introducción del protocolo MPLS no estaba muy clara cuál sería su función. Hoy en día han pasado a denominarse *Traffic Class* (Clase de Servicio) y se usan únicamente para el marcado de Calidades de Servicio (QoS *Quality of Service*) en todas las implementaciones.
- ***S (1 bit):*** El bit S indica la parte inferior de la pila (*Bottom of Stack*). Esto es, cuando existe apilamiento de varias etiquetas dentro de un mismo paquete, la etiqueta al final de la pila llevará este bit S a 1, mientras que el resto de etiquetas lo mantendrán a 0.
- ***TTL (8 bits):*** Este campo de la cabecera MPLS funciona igual que el campo TTL de la cabecera IP. El valor TTL se decrementa en cada salto a través de un LSR para prevenir que los paquetes pudieran mantenerse dando vueltas en un bucle de reenvío, infinitamente. Así, en caso de bucle en el reenvío, por lo menos, cuando el campo TTL llega a 0 el paquete es descartado.

2.5.5 Requerimientos para el control de procesos en MPLS

Con el fin de conseguir un entorno MPLS apropiado y un buen funcionamiento y operación del mismo, los *routers* de nuestro *backbone* de proveedor de servicios han de ser conscientes del resto de encaminadores y conocer el emplazamiento de cada FEC definido en ellos (entendiendo estos FECs como prefijos IP). Esta tarea se consigue cuando todos los routers corren un protocolo de enrutamiento escalable y optimizado para tal efecto (como OSPF o IS-IS).

Puesto que hablamos de protocolos de encaminamiento que correrán dentro del núcleo de la red, y que serán administrados bajo una misma compañía (definiéndose así un Sistema Autónomo), a este tipo de protocolos se les llama habitualmente *Interior Gateway Protocols* (IGP). Aunque no hablaremos en detalle sobre sus características, mencionaremos brevemente su operativa.

Después de que se establezcan las adyacencias o vecindades entre los encaminadores directamente conectados, entre ellos se intercambiará información que hará rellenar las tablas de rutas globales de cada uno de ellos.

Cada *router* intercambiará información acerca de sus enlaces con el resto de la red, gracias a la inundación de paquetes de actualización.

Tras la sincronización de las bases de datos de todos ellos, esto es, cuando el protocolo de enrutamiento haya convergido, los encaminadores dispondrán de los FECs presentes en el resto de *routers* indicándose éstos como entradas de tipo “remotas”, y las propias como entradas de tipo “local” en sus tablas de reenvío (FIB).

Llegados a este punto, el encaminamiento y reenvío de paquetes IP está operativo usando para ello las tablas IP de reenvío (FIB).

Como un punto adicional, no mencionado en esta breve descripción del funcionamiento de los protocolos de enrutamiento, diremos que éstos a veces han de ser capaces de llevar información adicional en sus paquetes de actualización, concerniente a la ingeniería de tráfico que se puede emplear con MPLS.

Resumiendo, el IGP es responsable de distribuir la información que necesitamos para saber alcanzar cada elemento a través de la red y de asegurar que los caminos se recalculan y optimizan tras cualquier evento de fallo en la infraestructura.

Para ser capaces de establecer los LSPs de MPLS (túneles) y habilitar así el reenvío de paquetes basado en etiquetas, el paso siguiente es el establecimiento de un mecanismo de intercambio entre encaminadores para dar a conocer las uniones etiqueta-FEC seleccionadas.

Tal mecanismo (protocolo) definirá el conjunto de reglas y procedimientos de cómo los *routers* intercambiarán las etiquetas y su interpretación. Se han estandarizado una serie de protocolos para tal efecto.

En los siguientes puntos nos centraremos en definir algunos principios de diseño que los protocolos de distribución (señalización) de etiquetas han de reunir.

2.5.6 Términos clave en Protocolos de Distribución de etiquetas

Antes de ahondar en el funcionamiento concreto los principales protocolos de distribución de etiquetas en MPLS desde la perspectiva del plano de control, hemos de describir y definir algunos términos clave que nos servirán para comprender la operativa particular de estos protocolos.

2.5.6.1 Río arriba, río abajo

Como pasa con muchos otros conceptos en un entorno MPLS, aquí la dirección en la que fluye el tráfico es clave, ya que de ella depende la definición de los conceptos "río arriba" (*Upstream*) y "río abajo" (*Downstream*).

A lo largo de este proyecto, en los ejemplos, asumiremos en muchas ocasiones que el tráfico fluye de izquierda a derecha, pero no hemos de olvidar que en la mayoría de casos el tráfico va en ambas direcciones, aunque por simplicidad, tengamos sólo en cuenta una de ellas.

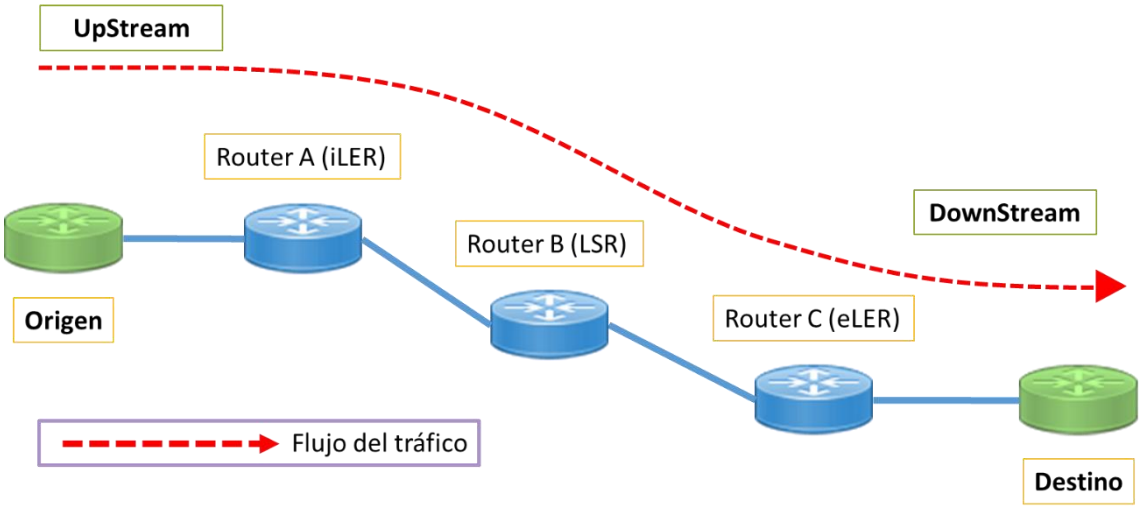


Figura 15: Flujo de Tráfico – Río Arriba/Río Abajo

Dicho esto, y a la vista de la figura 15, suponiendo que el CE a la izquierda es el origen del tráfico y el CE a la derecha es el destino del tráfico, definimos "encaminador río arriba" como aquel más cercano a la fuente (origen) en relación a otros. Así, la definición de ambos términos dentro de un mismo flujo puede acotarse al entorno o relación entre dos o más elementos.

La definición de "encaminador río abajo" pasa por tanto por decir que es aquel elemento más alejado de la fuente, o lo que es lo mismo en nuestro flujo, aquel más cercano al destino en relación a otros.

El flujo de tráfico por consiguiente siempre es transportado en dirección río abajo, desde un router *upstream* a un router *downstream*.

El plano de control (señalización) por su parte invierte este orden como veremos más adelante.

2.5.6.2 Modos en la distribución de etiquetas

Si deseamos usar el reenvío en base a etiquetas de MPLS, los encaminadores de la red primero han de generar y anunciar las etiquetas vinculadas a los FEC seleccionados. Con esto logramos rellenar las tablas de etiquetas que usaremos para el reenvío y definir los LSPs de una manera consistente. Para este propósito usaremos un protocolo de señalización MPLS común, que se habilitará en todos los routers participantes.

Sin embargo, la RFC 3031 [Ref.2] que define la arquitectura MPLS no establece el uso único de un protocolo de señalización. Además la propia RFC propone varias alternativas que definen las formas de distribuir y mantener las uniones etiquetas-FEC.

Por ello, en este apartado se explicarán los aspectos generales de los modos de distribución y de control y retención, para posteriormente cubrir en puntos específicos, los protocolos de señalización MPLS soportados por el portfolio de equipos Alcatel-Lucent Service Router y cómo implementan éstos los modos mencionados.

Existen dos métodos en el proceso de distribución de las uniones que identifican etiquetas con FECs:

- *Downstream Unsolicited* (DU) – Rio abajo no solicitado: El enrutador distribuye la unión etiqueta-FEC a sus vecinos en MPLS, sin que éstos pregunten acerca de dicha etiqueta. En otras palabras, el router decide anunciar la unión etiqueta-FEC sin importar si algún otro router la necesite o no.
- *Downstrem on Demand* (DoD) – Río abajo bajo demanda: En este modo el enrutador sólo distribuirá la unión etiqueta-FEC a otro enrutador si éste la solicitó previamente, de ahí la denominación “bajo demanda”.

Una vez las asociaciones etiqueta-FEC hayan sido anunciadas desde los routers de egreso, y reenviadas por los LSRs, las conexiones mediante etiquetas estarán completadas y los LSPs establecidos de origen a destino.

Los enrutadores construyen una base de datos con la información necesaria para el reenvío mediante etiquetas, denominada *Label Forwarding Information Base* (LFIB), basada en el mejor camino, usando el IGP o las rutas restringidas definidas (dependiendo de la configuración realizada y del protocolo escogido), hacia el destino.

Es ahora cuando el reenvío del tráfico de cliente se lleva a cabo mediante el uso de las etiquetas negociadas.

Una vez hemos definido los dos métodos en el proceso de distribución de etiquetas, tenemos que mencionar los métodos más utilizados para el control de los anuncios. Esto hace referencia al orden en que los nodos crean y anuncian las asociaciones o uniones etiqueta-FEC en la red. Como en el caso anterior, se definen dos modos principales en la práctica:

- *Ordered Control* – Control Ordenado: Cuando un enrutador actúa bajo este modo, sólo distribuirá una etiqueta para un FEC para el cual él mismo es el eLER

de dicho FEC o bien haya recibido de su *next-hop* (próximo salto) una etiqueta para ese FEC.

- *Independent Control* – Control Independiente: En este otro modo, el enrutador distribuye las etiquetas para los FECs que conoce hacia los routers *upstream*, sin importar si ha recibido una etiqueta de los routers *downstream* propietarios de los FECs. Esta manera de actuar es la forma en la que el enrutamiento IP convencional trabaja. Cada nodo decide de forma independiente con respecto a cómo tratar cada paquete, y confía en que los algoritmos de enrutamiento converjan rápidamente para que cada datagrama se entregue al destino correcto.

Para asegurar que el tráfico de un determinado FEC siga el camino con unas propiedades específicas y definidas (por ejemplo, evitar que el tráfico atraviese un nodo dos veces, o que el camino posea una cantidad de recursos de ancho de banda) hemos de usar el modo Control Ordenado (*Ordered Control*), ya que si utilizáramos el Control Independiente (Independent Control), los LSRs podrían empezar a reenviar tráfico de un FEC, usando las etiquetas, antes incluso de que el LSP se haya establecido completamente, lo que puede ocasionar que el tráfico del FEC siga un camino que carece de las propiedades específicas configuradas para ese tráfico y no se tengan en cuenta ciertas restricciones.

Por último definiremos los modos de retención, que definen cómo y cuándo los nodos almacenarán las etiquetas en memoria:

- *Liberal Retention* – Retención Liberal: En este modo los enrutadores almacenarán todas las etiquetas que reciban de otros enrutadores en la *Label Information Base* (LIB). [Nota: no confundir con la LFIB]. Este método permite adaptarse mejor a los cambios pero consume más recursos de memoria.
- *Conservative Retention* – Retención Conservadora: Los enrutadores que trabajan con este método comprueban las etiquetas recibidas de otros enrutadores, y sólo almacenan en sus bases de datos las etiquetas que consideran válidas. Este método consume menos recursos de memoria al almacenar menos cantidad de etiquetas, pero por el contrario es más lento en reaccionar cuando se producen cambios en el enrutamiento. [Nota: la consideración de validez de una etiqueta será expuesta cuando hablemos de cada uno de los protocolos de señalización/distribución de etiquetas].

Habiendo presentado ya los aspectos generales de los modos de distribución y de control y retención, sólo queda reseñar los usos de éstos en las implementaciones de protocolos. Aunque existen otras combinaciones posibles de uso, la mayoría de implementaciones usan una de las siguientes composiciones:

- *Conservative Retention* con *Downstream On Demand*
- *Liberal Retention* con *Downstream Unsolicited*

En nuestro caso particular, las combinaciones utilizadas en los equipos Alcatel-Lucent SR OS que utilizaremos en nuestro despliegue, son las mostradas en la tabla:

Protocolo	Modo de Distribución	Modo de Control	Modo de Retención
LDP	Downstream Unsolicited	Ordered	Liberal
RSVP	Downstream On Demand	Ordered	Conservative

Tabla 2: Combinaciones en los modos de distribución de etiquetas en base al protocolo

2.5.6.3 Espacio de etiquetas: Por Dispositivo o Por Interfaz

Existen dos tipos de espacios de etiquetas: por dispositivo y por interfaz.

El espacio de etiquetas por dispositivo asigna una etiqueta por FEC y por dispositivo o nodo, usada por todas las interfaces del equipo.

El espacio de etiquetas por interfaz por su parte, asigna una etiqueta única para cada FEC por interfaz, normalmente basándose en los recursos específicos de la interfaz, tales como el DLCI en Frame Relay o el VPI/VCI en ATM.

El espacio de nombre por dispositivo usa menos recursos en cuanto a etiquetas se refiere. Con este tipo de espacio de nombres, la misma etiqueta puede usarse para reenviar un paquete desde un LSR, sin importar el puerto físico que se use para reenviarlo. Es muy común en entornos de Ethernet.

Los routers de servicios de Alcatel-Lucent que usaremos en nuestro despliegue implementan este tipo de espacio de etiquetas.

2.5.7 Protocolos de señalización para etiquetas de transporte

Los dos principales protocolos para la distribución y el intercambio de etiquetas de transporte MPLS (etiqueta externa del paquete) son LDP (*Label Distribution Protocol*) y RSVP-TE (*ReSource reserVation Protocol with Traffic Engineering*), entendiendo estas etiquetas de transporte como aquellas que utilizamos para el reenvío de los paquetes de cliente que entrarán dentro de nuestra red IP/MPLS de proveedor de servicios.

Un breve acercamiento a sus características principales:

LDP crea LSPs basándose en la información obtenida del protocolo de encaminamiento IGP. La señalización e intercambio de etiquetas crean los caminos LSPs, determinados por el algoritmo usado por el IGP, normalmente SPF (*Shortest Path First*), implementado en OSPF e IS-IS. La selección de rutas que hace el IGP determina el mejor camino, que será el que usará el LSP para ese FEC. Cada router *downstream* elegirá de forma independiente la etiqueta que usará para reenviar el tráfico etiquetado hacia el destino.

LDP no proporciona redundancia ni mecanismos de protección más allá de los posibles múltiples caminos del propio protocolo IGP y del ECMP (*Equal-Cost Multi-Path*).

Obviamente es un protocolo con el que se simplifica mucho el despliegue, sobre todo si estamos en redes de operadores en el que el número de encaminadores es grande o se prevé que lo sea.

Por otra parte, RSVP-TE establece los túneles LSPs que habilitan la asignación de recursos a lo largo del camino definido, usando el camino elegido por el IGP o estableciendo un camino estricto definido a través de varios routers *downstream*. RSVP-TE posibilita la asignación de ancho de banda por camino LSP, permitiendo al encaminador a la entrada de la red (iLER) elegir qué camino es capaz de cumplir con los requerimientos y expectativas en cuanto al ancho de banda se refiere.

RSVP-TE es capaz de soportar también el establecimiento de LSP basándose en caminos elegidos por el IGP, usando un algoritmo basado en restricciones como el CSPF (*Constraint-based Shortest Path First*), o basándose en caminos definidos de manera explícita por configuración. Los protocolos IGP (OSPF o IS-IS) requieren de configuración adicional para poder aplicar el algoritmo CSPF.

RSVP-TE incluye además un conjunto de mecanismos de protección ante fallos en los enlaces y en los nodos, como son la creación de caminos secundarios y el re-enrutamiento rápido (*Fast Reroute*), que hacen que los tiempo de convergencia de red se vean ampliamente superados con respecto a los que manejan los protocolos IGP.

Como contrapartida, RSVP-TE precisa una configuración más compleja y exhaustiva en los nodos de la red, requiriendo normalmente un mallado de LSPs entre todos los PEs de la arquitectura, lo cual puede traducirse en la creación, dependiendo del número de equipos, de cientos de estos túneles de transporte.

2.5.8 Protocolos de señalización para etiquetas de servicios

Además de los protocolos de señalización mencionados anteriormente para el intercambio de etiquetas de transporte, los routers de Alcatel-Lucent utilizan otros protocolos de señalización que se usan y configuran habitualmente cuando estamos implementando servicios basados en tecnología MPLS. Estos son los denominados protocolos de señalización para etiquetas de servicios, y su objetivo primordial es el intercambio y distribución de las etiquetas asociadas a cada servicio definido (etiqueta interna del paquete) dentro de la pila de etiquetas MPLS. Es por ello que el propósito de éstos es completamente diferente al que tienen LDP o RSVP-TE.

El primero de estos protocolos es T-LDP (*Targeted LDP*), usado en servicios VPN de capa 2, y especificado en el RFC 4447 [Ref. 3]. Señaliza las etiquetas que identifican a un servicio en particular, desde el router de ingreso al de egreso, como puede ser un ePipe o una VPLS, creando una sesión extremo a extremo entre los mencionados routers de entrada y salida de la red.

El segundo de estos protocolos es MP-BGP (*Multiprotocol extensions to Border Gateway Protocol*), usado en servicios VPN (IP) de capa 3, y especificado en el RFC 4364 [Ref. 4].

Es una mejora del protocolo BGP para la señalización de etiquetas MPLS en los servicios VPRN (VPNs de capa 3).

2.5.9 Etiquetas MPLS de uso especial

Las etiquetas con valores entre 0 y 15 están reservadas para usos especiales y están relacionadas con aplicaciones especiales:

- Etiqueta 0: representa "*IPv4 Explicit NULL label*".
- Etiqueta 1: es la etiqueta de alerta del enrutador y no puede posicionarse en la parte inferior de la pila de etiquetas (*bottom of stack*).
- Etiqueta 2: representa "*IPv6 Explicit NULL label*".
- Etiqueta 3: representa "*Implicit NULL label*"
- Etiquetas 4-15: se reservan para su uso en el futuro.

Tanto la etiqueta *IPv4 Explicit NULL* como la *IPv6 Explicit NULL*, habían de situarse en la parte inferior de la pila, según lo indicaba el RFC3032 [Ref. 5]. Esta restricción en el posicionamiento de estas etiquetas fue eliminada en el nuevo RFC 4182 [Ref. 6].

El uso que le damos a las etiquetas 0-3 va a ser explicado y detallado en los siguientes puntos.

2.5.9.1 Implicit NULL Label

La siguiente figura ilustra la operación normal dentro de un LSP, en este caso con punto inicial Router 1 y que termina en el Router 3 conectado a la red W:

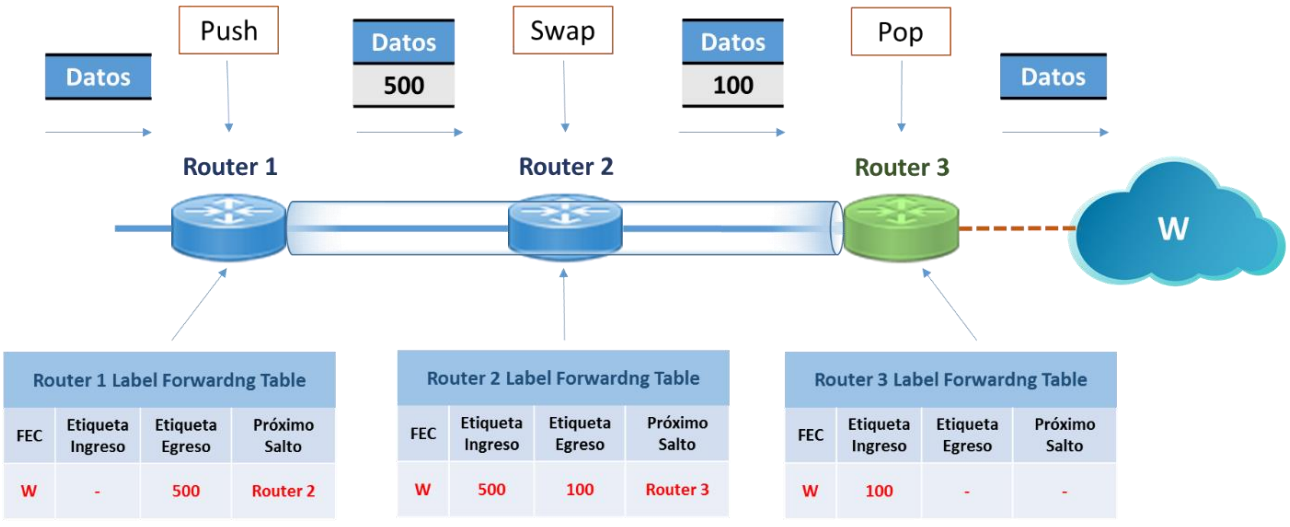


Figura 16: Operación estándar dentro de un LSP

Así, el Router 3 recibirá los paquetes procedentes del Router 2 con la etiqueta 100 para el FEC W. Es entonces cuanto el Router 3 eliminará la etiqueta de transporte 100, y enviará los datos originales del paquete hacia su destino, la red W.

Si utilizamos el anterior escenario como referencia, el Router 3 podría ahorrar recursos de procesamiento en CPU si éste no tuviera que llevar a cabo una búsqueda en la base de datos de las uniones etiqueta-FEC para W. Por tanto sería más práctico si Router 2 enviara los paquetes del FEC W sin etiqueta de transporte.

Para poder realizar este tipo de procesamiento, el Enrutador 3 señaliza esta petición al Enrutador 2 mediante el anuncio de la unión etiqueta-FEC esta vez usando el valor 3 para dicha etiqueta. Esto es lo que denominamos "Nulo Implícito" (*Implicit Null*).

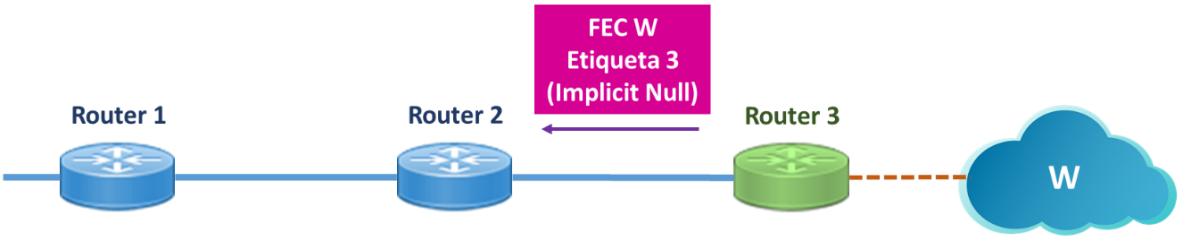


Figura 17: Etiqueta Implicit Null

El Router 2 guardará la etiqueta 3 como si de cualquier otra etiqueta se tratara, asociándola al FEC W.

A pesar de que el Router 2 no intercambiará (*Swap*) la etiqueta de los paquetes entrantes (con la etiqueta de egreso con valor 3), ya que la etiqueta de valor 3 nunca aparece en una cabecera MPLS, en su lugar el encaminador enviará el paquete sin etiquetar hacia el Router 3, el cual actuará, como en el modo normal, como un LER para el LSP (túnel). En este escenario el Router 3 es el último salto para el FEC W, lo que convierte al Router 2 en el penúltimo.

Cuando este penúltimo *Router* es el encargado de eliminar la etiqueta denominaremos dicho comportamiento como *Penultimate Hop Popping* (PHP).

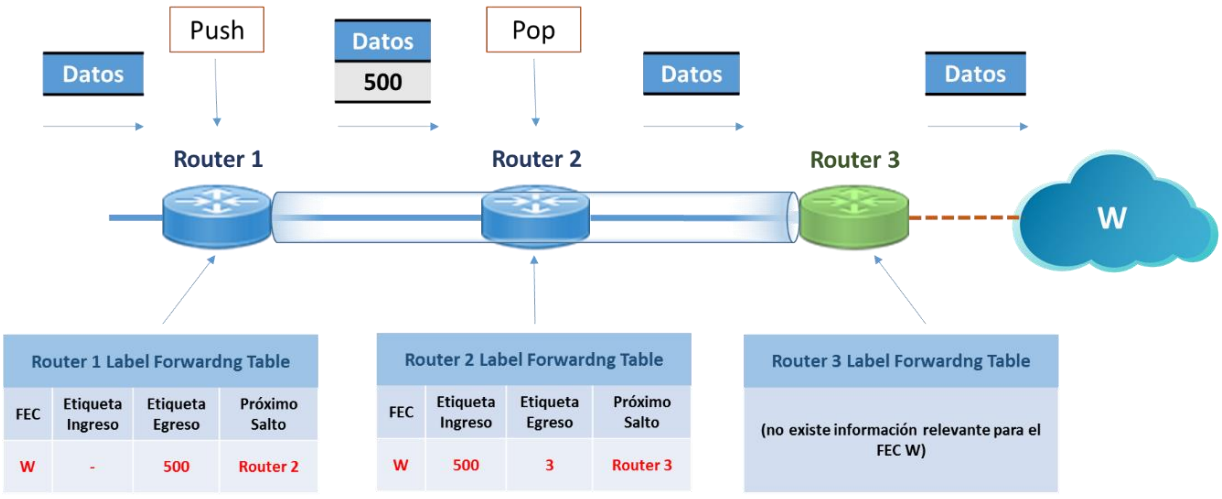


Figura 18: Comportamiento PHP – Penultimate Hop Popping

Es importante recalcar que el Router definido como penúltimo salto sólo elimina la etiqueta más externa de transporte, dejando la(s) restante(s) intacta(s) en la pila de etiquetas, para que el último salto tome la decisión del servicio a utilizar basándose en la etiqueta de servicio.

El principal beneficio de usar PHP es, como ya hemos mencionado, la optimización del rendimiento en el enrutador de egreso (eLER). Sin embargo, también existe una principal desventaja, y es que, al eliminar la etiqueta de transporte, cualquier información adicional en la cabecera MPLS se pierde, como pueden ser los parámetros de QoS de los bits EXP, lo que hará que el paquete pueda no recibir el tratamiento adecuado en el router de egreso de la red.

2.5.9.2 Explicit NULL Label

La etiqueta generada por el Router 3 (el enrutador de egreso para W) puede ser de valor 0, en cuyo caso se conoce como etiqueta de "Nulo Explícito" (*Explicit Null*).

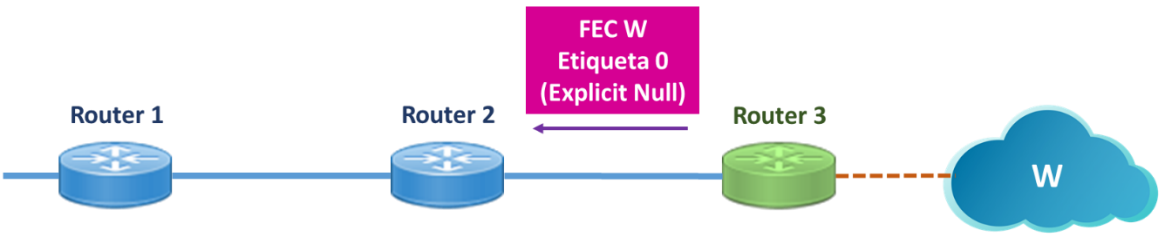


Figura 19: Etiqueta Explicit Null

Si el valor es 0 será *IPv4 Explicit Null* y si es 2 será *IPv6 Explicit Null*.

Esta etiqueta *Explicit Null* solventa el problema de PHP con el que perdíamos los parámetros de QoS en el campo EXP de la cabecera MPLS. El Router 2 (penúltimo enrutador) reenvía el paquete con la etiqueta de valor 0 (ó 2 para IPV6). De esta forma mantenemos el valor del campo EXP. El eLER podrá tratar entonces el paquete en base al campo de QoS (EXP), antes de eliminar la etiqueta y reenviar el paquete a la red de destino consecuentemente. La eliminación de la etiqueta se realiza directamente, sin hacer búsqueda en la base de datos de etiquetas.

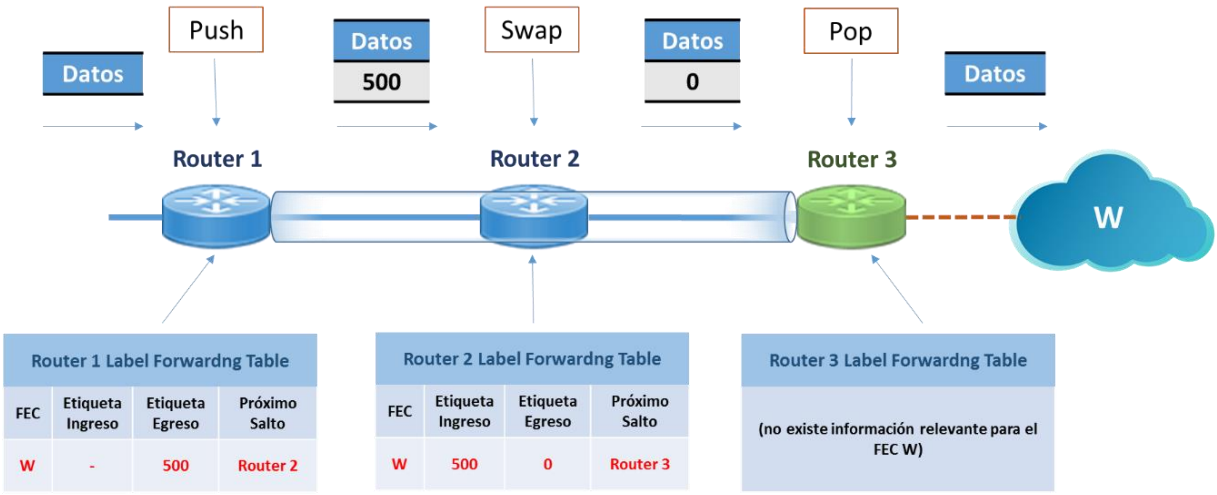


Figura 20: Solución al problema en PHP con la etiqueta Explicit Null

En nuestro caso particular y para nuestro despliegue, mencionar que los SR OS de Alcatel-Lucent siempre han soportado las peticiones de *Explicit Null*. Sin embargo como enrutadores eLER no se contempla el envío de peticiones de *Explicit Null* ya que el rendimiento no se ve afectado. No es un problema en estos routers.

2.5.9.3 Router Alert Label

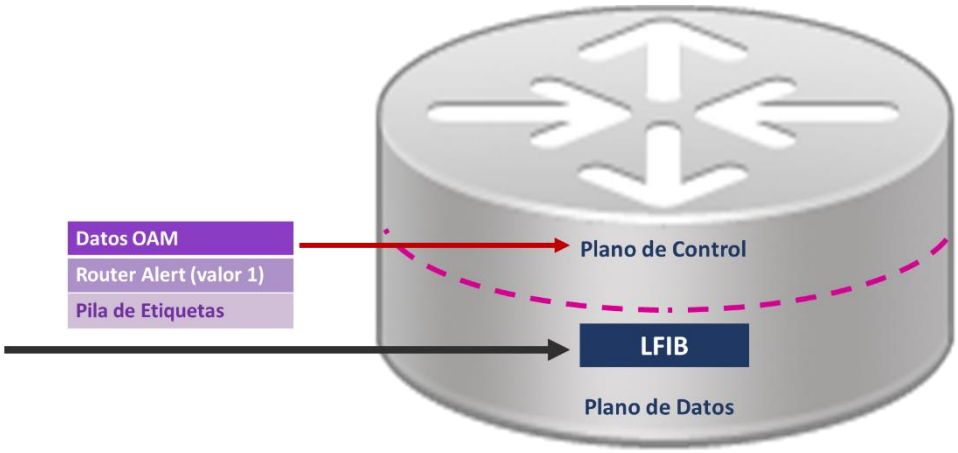


Figura 21: Etiqueta de Alarma para Herramientas OAM

La etiqueta con el valor 1, se corresponde con la etiqueta de "*Router Alert*" usada en ciertas aplicaciones de OAM (Operational, Administration, Maintenance). Algunos de estos comandos OAM requieren el uso de esta etiqueta especial (tales como MAC-ping o el SDP-ping).

El router que envía dichos comandos inserta una etiqueta "*Router Alert*" con el valor 1, de tal forma que el router receptor del paquete des-encapsula y procesa la cabecera de MPLS en el Plano de Datos (Plano de Reenvío). Inmediatamente se da cuenta de que la información del paquete debe conducirse internamente al Plano de Control en lugar de

reenviarse a otra interfaz física. Finalmente el mensaje OAM es procesado por el Modulo de Control que tomará las acciones precisas.

2.6 Introducción a *Label Distribution Protocol* (LDP)

Como ya se ha mencionado anteriormente, LDP es un protocolo destinado a la distribución de etiquetas en MPLS. Se define dentro del RFC 3036 [Ref. 7] y fue actualizado por el RFC 5036 [Ref. 8]. Aquellos enrutadores que corren LDP establecen sesiones con otros equipos que corren también LDP. Estas sesiones permiten el intercambio de información acerca de las uniones etiqueta-FEC, denominado en ocasiones "mapeo".

Para llevar a cabo la conmutación y reenvío de paquetes en un entorno de MPLS, es necesario que los routers de nuestra red de proveedor de servicios distribuyan dichas etiquetas para los distintos FECs (prefijos IP) que aparezcan en sus tablas de rutas (FIB). LDP se introdujo para llevar esta información, etiqueta-FEC, sin importar el protocolo de enrutamiento que se use en la red, ya que la modificación de dichos protocolos para llevar la información de mapeo se tornaba algo complicada debido a la variedad y cantidad de los mismos (RIP, OSPF, IS-IS, etc.)

En particular, en los productos de la familia Alcatel-Lucent SR usamos el protocolo LDP para:

- Establecer los Túneles de Transporte, LSPs.
- Establecer las "Sesiones LDP Dirigidas" (*Targeted LDP Sessions*) entre los equipos conectados directa o indirectamente, necesarios para la creación de los "Túneles de Servicio".

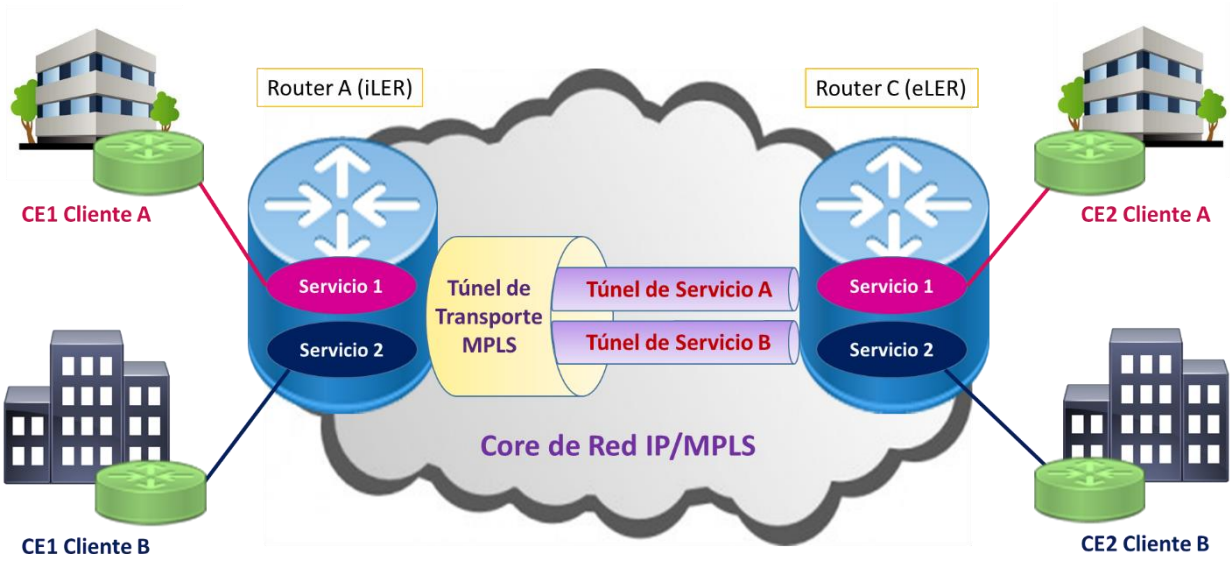


Figura 22: Túneles de Transporte y Servicio en arquitecturas de interconexión de sedes

En este ejemplo (Figura 22), puede apreciarse cómo los túneles MPLS pueden usarse para la creación de servicios punto a punto.

Solamente los PEs, o routers de borde de la red MPLS, tienen constancia de los servicios. De modo que la configuración de estas instancias de servicio ha de hacerse en todos aquellos routers PE que participen en la VPN de cliente. Así, un único conjunto de túneles de transporte, pueden llevar tráfico de cientos de instancias de servicios punto a punto, ya que para estos túneles de transporte, el tráfico de los diferentes servicios no es más que carga útil a transmitir.

Las instancias de servicio que se configuran en los equipos de borde son entidades virtuales (software) en los encaminadores de servicios. Debido a que cada instancia (entidad virtual) de servicio se maneja de forma separada a las demás, conseguimos proporcionar inherentemente un aislamiento entre clientes (cada uno asociado a una instancia), proporcionando seguridad y ajustes personalizados, así como la posibilidad de gestionar los recursos según necesidades, de manera más granular. El hecho de manejar los servicios de cliente de manera aislada ayuda a mejorar la escalabilidad de la red, lo cual es importante en los entornos de proveedor, en los que la visión a largo plazo se hace absolutamente necesaria.

2.6.1 Visión general y Operativa del Protocolo LDP

Toda sesión asociada a un "enlace LDP" (*Link LDP session*) se crea entre encaminadores conectados directamente (Figura 23). Tras establecerse el "enlace(s) LDP" (sesión), los routers intercambiarán sus vínculos (mapeos) etiqueta-FEC, y mantendrán "viva(s)" la(s) sesión(es) por medio del intercambio periódico de mensajes (*keepalives*).

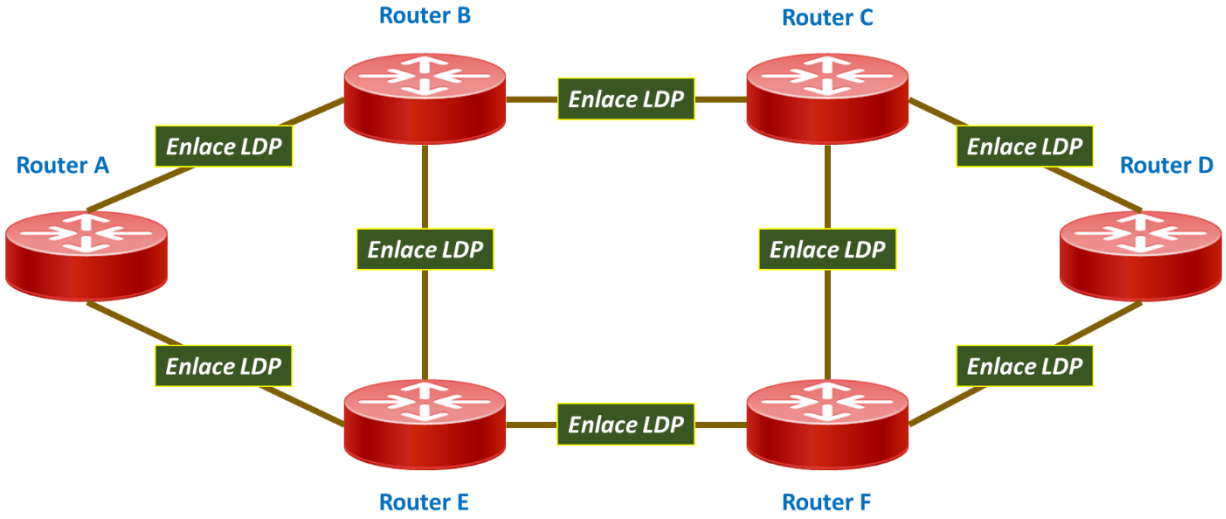


Figura 23: Enlace LDP (Link LDP)

El intercambio de etiquetas se realiza de forma muy similar a como trabajan los protocolos de encaminamiento (IGP). Se lleva a cabo un proceso de selección con las etiquetas recibidas para decidir cuál será el siguiente salto y qué etiqueta se usará para alcanzar los otros LSRs (*Label Switching Routers*). Así conseguimos que los LSPs (túneles)

se generen entre cada posible origen-destino conformando un mallado completo de la arquitectura LDP.

Nota: El protocolo LDP confía y necesita de la configuración de un protocolo IGP para el establecimiento de sus sesiones, obtener la información de los FEC y mantener los túneles LSPs creados.

Enumeraremos ahora los procesos principales para la creación y mantenimiento de sesiones LDP, que se detallarán posteriormente en puntos subsiguientes:

- **Descubrimiento de pares (*Peers Discovery*):** Es el primer proceso necesario para el establecimiento de sesiones en LDP y se realiza mediante el uso de mensajes "Hello", siendo un proceso similar al que ejecuta el protocolo de enrutamiento OSPF. Cada router envía uno de estos mensajes "Hello" por las interfaces de red en las que tiene habilitado LDP, usando como destino una dirección multicast (224.0.0.2) y un puerto "bien conocido" (646) del protocolo de transporte UDP.
- **Establecimiento y Gestión de sesiones (*Session Establishment & Management*):** Tras la fase anterior se crea una sesión entre los pares (*routers*), sin importar si entre ellos existe más de un enlace a nivel de red. Una vez descubiertos unos a otros (con sus mensajes Hello y acuses de recibo correspondientes) y habiendo establecido las sesiones, enviarán de forma periódica mensajes Hello para mantener la adyacencia intacta.
- **Gestión de Etiquetas (*Label Management*):** El propósito de LDP es distribuir etiquetas, y es gracias a las sesiones establecidas y usando los denominados "mensajes de mapeo de etiquetas" (*label mapping messages*) como puede llevarse a cabo este objetivo.
- **Notificaciones *(Notifications*):** En ocasiones uno de los FEC (prefijos IP) para los que se generó una etiqueta asociada, deja de estar disponible (p.ej. cambios en la configuración del equipo). Si esto ocurre, el *router* de egreso debe advertir a sus *peers* de que eliminen la etiqueta asociada que se distribuyó. Para ello se usa un "mensaje de retirada de etiqueta" (*label withdraw message*) que debe ser confirmado (ACK) por los routers que lo reciben usando un "mensaje de liberación de etiqueta" (*label release message*).

En base a lo descrito anteriormente, se definen dentro de LDP cuatro tipos/categorías de mensajes, organizados según el protocolo de transporte que utiliza cada categoría:

- ✓ **Mensajes basados en UDP**:
  - *Mensajes de descubrimiento*: Anuncian y mantienen a los router LDP en la red.
- ✓ **Mensajes basados en TCP**:
  - *Mensajes de sesión*: Establecen, conservan y terminan las sesiones entre *peers*.
  - *Mensajes de anuncio*: Crean, modifican y eliminan los mapeos de etiqueta-FEC.
  - *Mensajes de notificación*: Informan sobre eventos y errores acontecidos.

Nota: El uso de TCP se ve justificado por la necesidad de LDP de que la entrega de mensajes se lleve a cabo de forma ordenada y confiable para una correcta operación del protocolo.

2.6.2 Descubrimiento de Pares

Tras haber llevado a cabo una configuración previa de los routers que formarán parte de la arquitectura LDP dentro de la red MPLS, que pasa por crear las interfaces IP, definir una dirección IP de sistema (*System IP address*), y configurar y habilitar un protocolo de *routing* IGP, los enrutadores comenzarán entonces a intercambiar paquetes que relacionaremos con distintos procesos/fases del protocolo LDP.

Nota: Cómo configurar las interfaces IP de cada puerto y la *System IP address* (y el porqué de la importancia de ésta) se detallará exhaustivamente en el Capítulo 3, destinado, en parte, al despliegue de nuestra solución de proveedor de servicios.

La primera de las fases para el intercambio de información de etiquetas-FEC con LDP es el proceso que da nombre a este punto: Proceso de Descubrimiento de Pares (*Peer Discovery Process*).

Como ya se mencionó anteriormente, este proceso es muy similar al que ejecutan protocolos de enrutamiento IGP como OSPF o IS-IS.

Habiendo incluido las interfaces oportunas en el protocolo LDP y estando habilitado éste, el *router* comenzará enviando paquetes LDP Hello con el fin de descubrir a sus vecinos en ese segmento de red. Estos mensajes se envían a la dirección multicast reservada 224.0.0.2 y puerto UDP 646. Así, si varios de los encaminadores se encuentran dentro del mismo segmento (dominio de *broadcast*) todos recibirán los mensajes LDP Hello, aunque sólo procesarán el mensajes aquellos *routers* que tengan habilitado LDP en la interfaz que los conecta al mencionado segmento de red.

Nota: La dirección IP de origen en los paquetes LDP Hello es la de la interfaz de egreso del router que envía el mensaje.

La recepción de un mensaje LDP Hello en una interfaz indicará e identificará una adyacencia (de tipo Hello) con un potencial par ("*Link LDP peer*"), así como el espacio de etiquetas que el par tiene intención de usar.

A continuación se presentarán los parámetros más importantes de todos los que se incluyen en un mensaje LDP de tipo Hello.

Nota: Los procesos se irán explicando y exponiendo usando como ejemplo (Figura 24) un par de enrutadores de la anterior arquitectura de referencia LDP. Sin embargo, la misma secuencia de pasos y eventos se dan en cualquier otro par de routers adyacentes dentro de la topología.

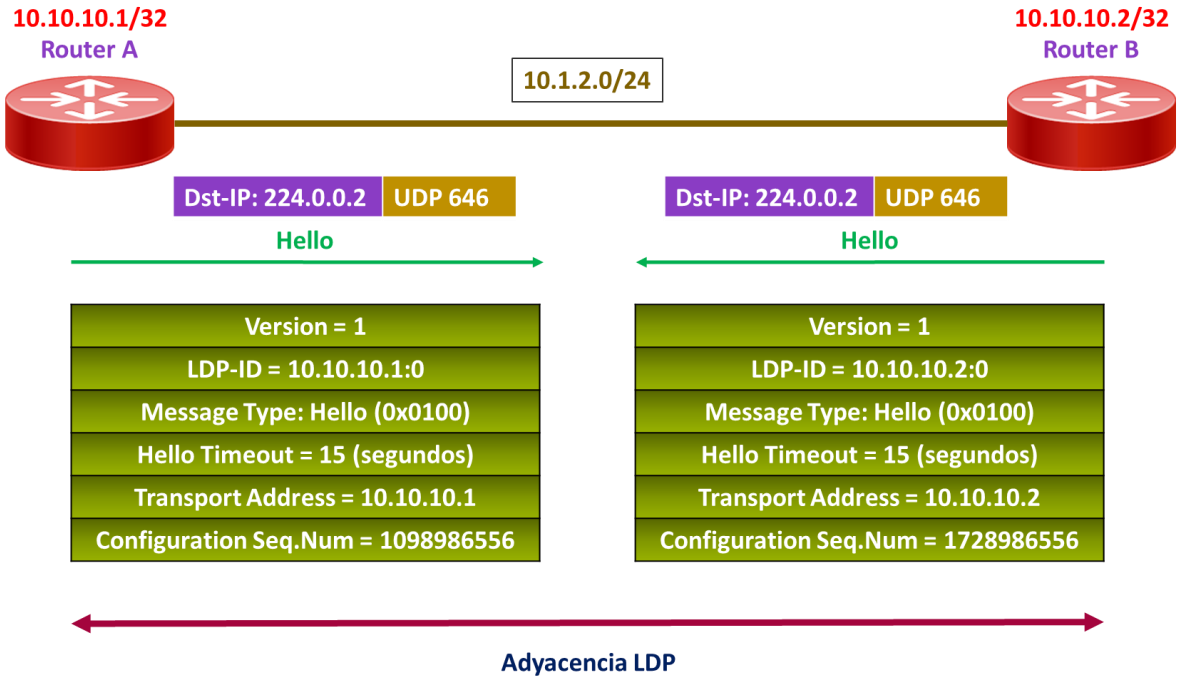


Figura 24: Paquetes Hello y Adyacencia en LDP

- ***LDP-ID***: Campo de 6 bytes de longitud que tiene como fin el identificar unívoca y globalmente al LSR y a su espacio de etiquetas. Los primeros 4 octetos (LSR ID) identifican al LSR, y típicamente se corresponden con la dirección IP del sistema (*System IP address*). En cuanto a los dos últimos octetos, éstos identifican el espacio de etiquetas que usará el LSR. En el caso concreto de los Routers de Servicio de Alcatel-Lucent, se usa un único espacio de etiquetas por plataforma, y no por interfaz (expuesto anteriormente), por lo que estos octetos siempre presentan el valor 0.
  Cuando un router LSR usa el protocolo de LDP para anunciar más de un espacio de etiquetas hacia uno de sus *peers*, han de establecerse tantas sesiones LDP como espacio de etiquetas se quieran anunciar (en este caso por tanto, los últimos dos octetos del LDP-ID para los espacios de etiquetas por interfaz no serán 0).

- ***Hello Timeout***: Aunque normalmente ante problemas que puedan surgir en el enlace entre peers, los protocolos de capas inferiores ya implementan mecanismos de detección y aviso de errores a capas superiores, para evitar fallos no detectados por dichas capas inferiores, LDP implementa un mecanismo de envío periódico de mensajes Hello. Estos mensajes se envían de forma continuada y periódica a los vecinos, en intervalos de tiempo prefijados por configuración (Figura 25). Todo encaminador espera recibir un mensaje Hello dentro del periodo definido en el *Hello Timeout* operativo, acordado durante el establecimiento de la Adyacencia Hello LDP. El valor por defecto para este campo

es de 15 segundos, pero puede personalizarse a nivel global, para que todas las interfaces LDP utilicen el mismo, o por interfaz, sobrescribiendo el valor global en la interfaz en la que se define.

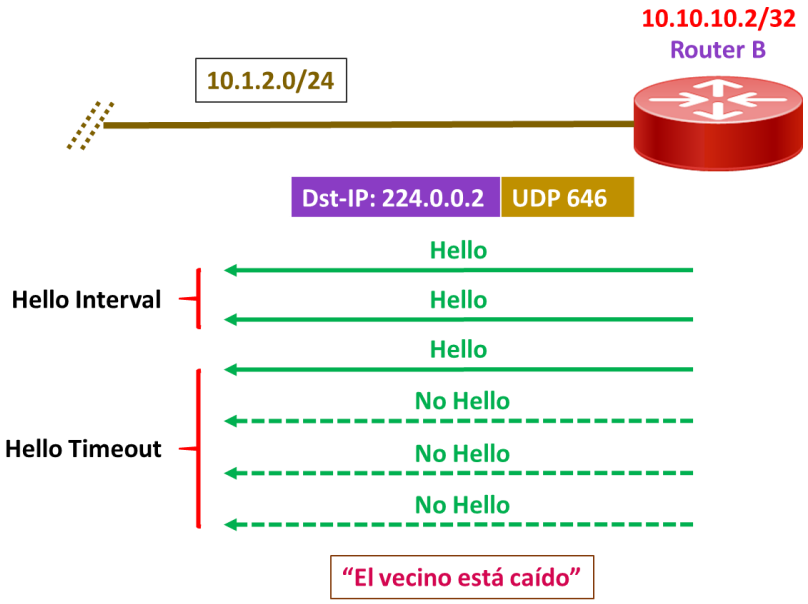


Figura 25: Parámetros temporales configurables en paquetes "Hello"

Para determinar cada cuanto tiempo se enviarán estos mensajes Hello, ha de establecerse el "*Hello factor*", esto es, cuántos mensajes se enviarán dentro del periodo de tiempo definido en el *Hello Timeout*. Este parámetro puede configurarse igualmente de manera global o por interfaz, y por defecto toma un valor de 3 en nuestros *routers*. Resumiendo; si queremos saber el intervalo de tiempo entre mensajes Hello, sólo hemos de dividir el *Hello Timeout* entre el *Hello factor*, esto nos proporcionará el denominado "*Hello Interval*".

Nota: Los valores del *Hello Timeout* no necesariamente han de coincidir en ambos routers que intentan formar una adyacencia durante el proceso de descubrimiento. El valor operacional para el *Hello Timeout* se negocia intrínsecamente, estableciéndose el menor de los valores, comparando el enviado con el recibido. Para determinar así el "*Hello Interval*" será necesario dividir el *Hello timeout* operacional (negociado) entre el *Hello factor* configurado localmente en el router.

- ***Transport Address***: Para realizar el intercambio de mensajes que anuncien las etiquetas tras la adyacencia, los *routers* necesitan de *sesiones LDP*, y éstas a su vez necesitan del establecimiento de conexiones TCP en las que correr.
  Es aquí donde tiene sentido el parámetro *Transport Address*. Será la dirección que el enrutador utilizará para llevar a cabo el proceso de establecimiento de sesiones LDP. El router puede elegir usar la dirección IP directamente conectada

(de la interfaz) o la dirección IP de sistema (*System IP address*) para usarse como *Transport Address*.
En nuestro caso particular, los Alcatel-Lucent Service Routers utilizan la "*System IP address*" como *transport address* por defecto, aunque puede modificarse de nuevo tanto a nivel global como por interfaz.
Se detallará en profundidad el proceso de establecimiento de sesiones en la siguiente fase del protocolo.

- ***Configuration Sequence Number***: Es un campo de 4 bytes que especifica un número de secuencia que hace referencia al estado de configuración del router. El router emisor del mensaje incrementa el número de dicho campo siempre que se produce un cambio en la configuración, como puede ser la modificación del parámetro "*Hello Timeout*". Gracias a este número el receptor del mensaje puede detectar cambios/modificaciones en la configuración LDP de su vecino.

2.6.3 Establecimiento de Sesiones LDP

Figura 26: Necesidad de Sesiones LDP

Como ya se ha mencionado, para realizar el intercambio de mensajes que anuncien las etiquetas y tras la adyacencia lograda en la fase anterior, los routers necesitan de sesiones LDP. Estas sesiones LDP a su vez necesitan del establecimiento de conexiones TCP en las que correr. La *Transport Address*, intercambiada como parámetro en los mensajes Hello, determinará:

- Qué enrutador inicia la sesión TCP (el *router* con la dirección de transporte mayor asume el rol de activo e inicia la conexión). El puerto usado como destino en estas conexiones a nivel de transporte TCP será siempre el puerto 646.
- Qué dirección IP usará el *router* para establecer la sesión.

Como ya se advirtió, los Alcatel-Lucent Service Routers utilizan la "*System IP address*" como *Transport Address* por defecto, aunque puede modificarse, de nuevo, tanto a nivel global como por interfaz.

Se han de tener en cuenta ciertas consideraciones cuando nos encontramos con enlaces múltiples entre encaminadores, esto es, más de un enlace entre ellos.

Ya hablamos del espacio de etiquetas en puntos anteriores (2.5.6.3 Espacio de etiquetas: Por Dispositivo o Por Interfaz). No se mencionó sin embargo, que existen dos tipos de implementaciones MPLS complementarias al concepto de espacio de etiquetas, denominados Modo Celda y Modo Trama. Estos dos modos definen cómo la etiqueta es transportada en función de la tecnología que usamos en el enlace.
El valor de la etiqueta MPLS puede ser transportado insertando la etiqueta en la cabecera del protocolo de nivel 2 (ejemplo de ello sería el caso de Ethernet) denominado Modo Trama, o bien utilizando uno de los campos de la cabecera del protocolo para indicar el valor de la etiqueta (ejemplo de ello serían ATM o Frame Relay, donde el campo VPI/VCI o DLCI respectivamente, de la cabecera, albergaría la etiqueta MPLS) denominado Modo Celda.

En el caso concreto de los enrutadores de servicios de Alcatel-Lucent este último modo (Modo Celda), no está soportado, pero su mención es relevante igualmente.

Es por esto que si dos enrutadores tienen entre sí interfaces que usan modo trama (Ethernet por ejemplo), el mismo conjunto de etiquetas se envían para los prefijos IP en ambas interfaces. Los valores para las etiquetas se obtienen de un conjunto común de etiquetas, que identificamos con el ya mencionado espacio de nombres por dispositivo/plataforma. Así, ambos routers mantendrán una única sesión LDP a través de las dos interfaces.

Si por el contrario las interfaces que los unen usan modo celda (ATM, o Frame Relay), se necesitará enviar etiquetas separadas por cada interfaz. Cada unión etiqueta-FEC en este caso es relevante para cada interfaz, usándose de hecho un espacio de etiquetas por interfaz. En este caso se requiere que ambos routers mantengan dos sesiones LDP separadas (lo mismo sería necesario si existiera una combinación de interfaces modo celda y modo trama entre ambos)

En el desarrollo de este proyecto, sólo se utilizarán interfaces en modo trama, y usaremos un espacio de etiquetas por dispositivo/plataforma, dado que es la implementación soportada por nuestros routers de servicios de Alcatel-Lucent.
En base a esto, una única sesión LDP es suficiente aun cuando haya múltiples enlaces entre los enrutadores, para habilitar los anuncios del conjunto común de etiquetas para los FECs seleccionados en cada router.

Esta sesión LDP requiere del uso de una dirección IP única y exclusiva como *Transport Address*, contra la que levantar la conexión de transporte TCP sobre la que correrá la sesión, como ya se indicó. En este punto podemos pensar que la sesión levantará sin problemas, habiendo definido las direcciones IP asociadas a cada interfaz del router y

habiendo intercambiado las direcciones de transporte en los mensajes que nos dieron la adyacencia (*Hello*).

Sin embargo y debido a que la dirección IP de sistema (*System IP address*) usada por defecto como Transport Address por los enrutadores Alcatel-Lucent se asigna a una interfaz especial denominada interfaz "*system*", sin puerto físico asociado (esto es, una interfaz de loopback especial) ésta no es visible por los routers adyacentes LDP si no es exportada a través de un protocolo de enrutamiento.

De hecho, la configuración y habilitación de un protocolo IGP de enrutamiento es una práctica común en los pasos a seguir antes de desplegar una red IP/MPLS de operador/proveedor de servicios, habitualmente antes de configurar el propio protocolo LDP.

Es tremendamente importante resaltar de igual manera, que el protocolo de enrutamiento no sólo es imprescindible para informar acerca de la *System IP address* de los "*peers*" que se usa como Transport Address, sino que también es necesario para la distribución de información sobre los prefijos IP (FECs) a lo largo de la red.

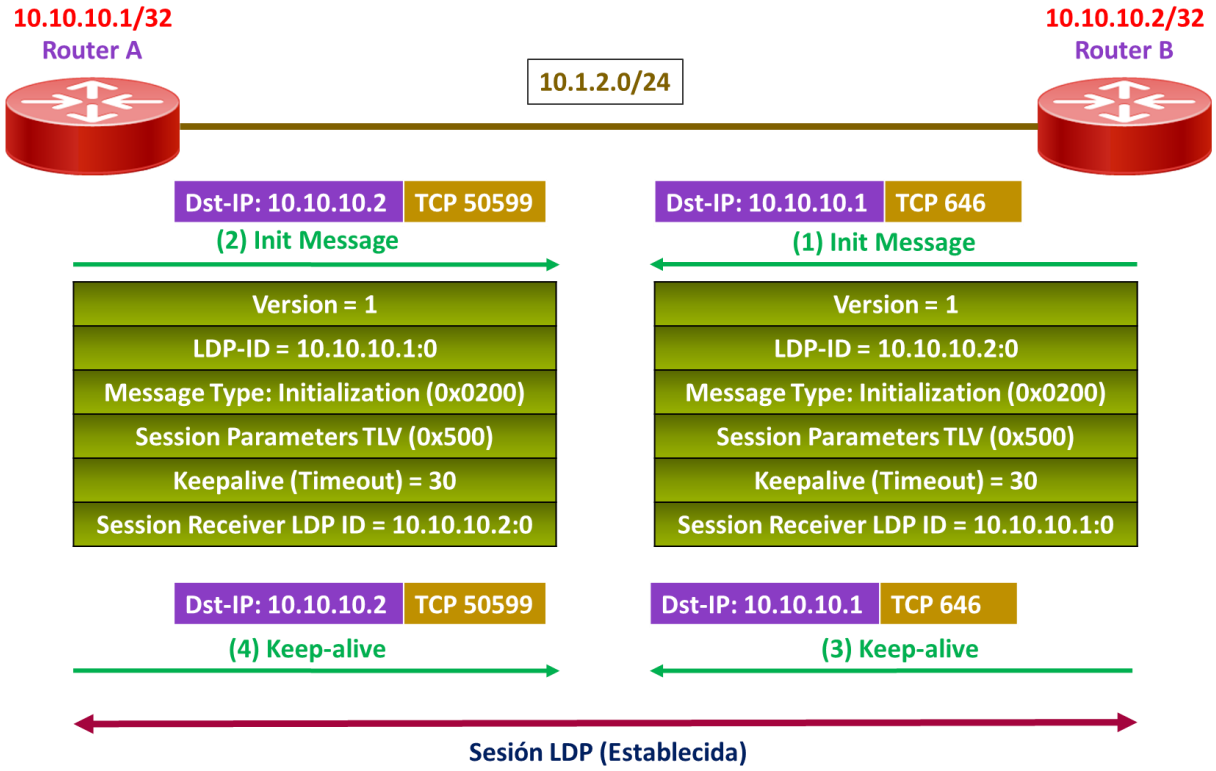


Figura 27: Mensajes Init y Establecimiento de Sesiones LDP

El enrutador con la dirección de transporte (*Transport Address*) más alta iniciará el proceso de establecimiento de la sesión LDP, véase la Figura 27. La petición de inicio de sesión se efectuará a través del denominado *Init Message* (Mensaje de Inicialización) hacia el puerto TCP destino 646 del router adyacente, y usando un puerto de origen elegido al azar, dentro del rango de los puertos dinámicos/privados de TCP (49152-65535) especificados por el organismo IANA.

Nota: En la Figura 27 anterior no se incluyen los detalles de la conexión TCP.

Dentro de la información incluida en el mensaje "Init" se encuentran parámetros como la versión del protocolo, el identificador LDP del enrutador origen del mensaje (campo del cual se habló previamente), el *Keepalive timeout* (que se describirá con posterioridad) o la identificación del receptor del mensaje.
Como puede observarse de nuevo en la Figura 27, la sesión no se establece hasta que el encaminador no recibe el mensaje *keepalive* de su vecino en respuesta al enviado.
Después de establecida la sesión, los enrutadores continuarán enviando mensajes *keepalive* esperando recibir los de su vecino.

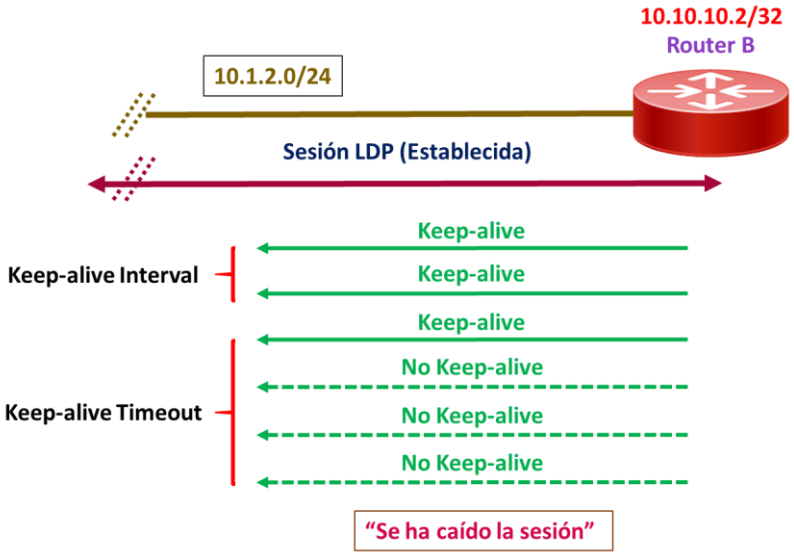


Figura 28: Parámetros temporales configurables en Paquetes Keep-alive

La configuración y operación de este mensaje en cuanto al *timeout* se refiere, es la misma que la que vimos para el caso de los mensajes periódicos de Hello, véase Figura 28.

Los valores del *Keepalive Timeout* no necesariamente han de coincidir en ambos routers para que la sesión se establezca. El valor operacional para el *Keepalive Timeout* se negocia intrínsecamente, estableciéndose el menor de los valores, comparando el enviado con el recibido. Para determinar así el "*Keepalive Interval*" será necesario dividir el *Keepalive Timeout* operacional (negociado) entre el *Keepalive factor* configurado localmente en el router.

2.6.4 Anuncio de Etiquetas

Una vez creadas las Sesiones en los Enlaces LDP, ahora sólo resta intercambiar las etiquetas para los FEC seleccionados. Recordemos que en el contexto que nos ocupa, un FEC no es más que un prefijo IP dentro de la tabla de rutas de nuestros dispositivos.

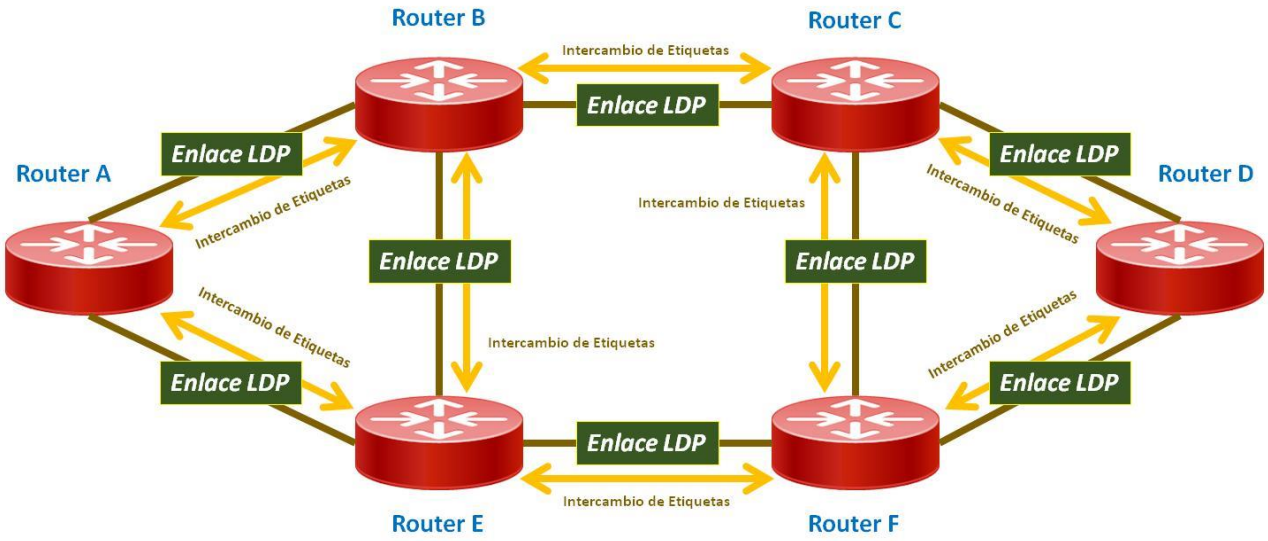


Figura 29: Intercambio de etiquetas mediante LDP

Dentro de un entorno de proveedor de servicios, como es el caso de este proyecto, en una red de servicios IP/MPLS, los túneles de transporte se utilizan para llevar el tráfico de servicios VPN. De este modo, cada router de la red sólo necesita conocer cómo alcanzar a los otros elementos, usando para ello la etiqueta asociada. Para llevar a cabo esto es suficiente que los enrutadores anuncien e intercambien las etiquetas para sus direcciones IP de sistema.

Como ya se definió, la dirección IP de sistema (*System IP address*) es la establecida para la interfaz de sistema (*System Interface*) que, como dijimos, es una interfaz de *loopback* especial, generada automáticamente en los routers de servicio de Alcatel-Lucent, y usada por defecto en muchos de los procesos que rigen el comportamiento del *router*.

Esta interfaz ha de estar accesible en tanto en cuanto el enrutador esté operativo, incluso si una interfaz física cae. Puesto que otros elementos de red deben de ser capaces de alcanzar la "*System Interface*" a través de otra interfaz física (principal característica de las interfaces de *loopback*), ya que no se encuentra vinculada a ningún puerto físico.

Así, el comportamiento por defecto de los Alcatel-Lucent Service Routers que usaremos en nuestro despliegue, es generar una única etiqueta para su "*System IP Address*" (FEC), y distribuirla a sus "*peers*" directamente conectados, usando las sesiones LDP activas.

Cuando los *peers* reciben el anuncio de la etiqueta, generan a su vez su propia etiqueta para la unión etiqueta-FEC correspondiente al prefijo recibido, y reenvían esta información al resto. De esta forma, las uniones etiqueta-FEC se distribuyen en la forma

en que lo harían los anuncios de rutas en los protocolos IGP, por inundación, aunque como es de esperar LDP posee mecanismos para evitar bucles durante el proceso.

Como resultado de este proceso de intercambio de etiquetas, cada *router* posee (al menos) una unión "etiqueta-*System_IP_Address*" de cada enrutador que compone la red.
Podemos así, de manera lógica, representar un LSP como la secuencia de etiquetas que se usa desde el ingreso en un punto de la red hasta el egreso en otro punto junto con las acciones tomadas sobre esas etiquetas (*Push*, *Swap*, *Pop*).
Se consigue de esta forma un mallado completo de túneles de transporte, que permitirá la comunicación basada en etiquetas entre cualesquiera dos entidades de la red IP/MPLS.

Como apunte final a este apartado, ha de tenerse en cuenta que, usando LDP, el enrutador no tiene visibilidad extremo a extremo de los túneles, sino que sólo sabe cuál es la etiqueta de salida que ha de utilizar y el router designado como *next-hop* para alcanzar el destino del túnel. Información ésta derivada de la pertinente entrada en la tabla LFIB. Por lo tanto, usando túneles de transporte señalizados mediante LDP, un LSP no es más que una "construcción lógica" de un túnel real extremo- extremo.

2.6.5 Distribución adicional de prefijos mediante políticas de Exportación.

Los routers de servicios Alcatel-Lucent distribuyen una única unión etiqueta-FEC, la correspondiente a la *System IP Address*. Sin embargo es posible generar más etiquetas, para cada prefijo local, por ejemplo, y que éstas se distribuyan igualmente por la red.
Cuando hablamos de prefijo local nos referimos a aquel prefijo propiedad del *router* en sí, una interfaz que se configuró directamente en ese enrutador. Esto puede ser, una interfaz que esté directamente conectada al equipo, o una interfaz de loopback, igual que la "*System interface*".
Estos prefijos adicionales se distribuirán gracias a la configuración y aplicación de políticas de exportación en LDP, como se muestra en la Figura 30.

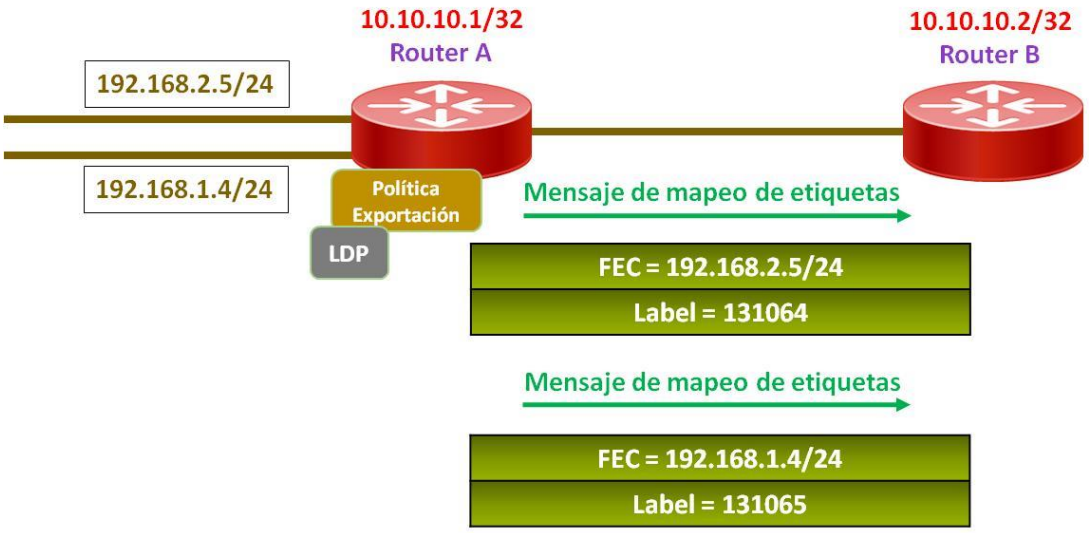


Figura 30: Políticas de Exportación en LDP

Una política puede definirse como una plantilla que permite al administrador imponer control adicional sobre la operación normal de un protocolo o funcionalidad del equipo. Estas policitas pueden estar compuestas por múltiples entradas, cada una de las cuales representa una condición de coincidencia, junto con una acción a llevar a cabo si la coincidencia se da. Estas condiciones se definen de forma diferente dependiendo del protocolo al que se apliquen, así como del propósito que tengan.
Si hay múltiples entradas, éstas irán secuenciadas por un número que indicará el orden en el cual se evaluarán, comenzando por el número más bajo. Se mostrarán ejemplos de políticas y configuración en el apartado de configuración del capítulo 3 de este proyecto.

2.6.6 Rechazo de uniones etiqueta-FEC mediante políticas de Importación

Por defecto, los routers de servicio de Alcatel-Lucent aceptan cualquier unión etiqueta-FEC que reciben de sus *peers*.
Este comportamiento puede modificarse, como ocurría en el anterior punto, mediante una política, sólo que en esta ocasión la política es de importación.

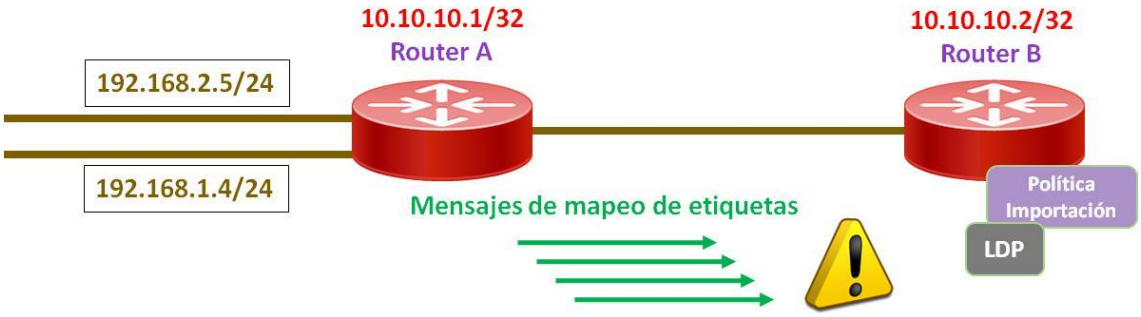


Figura 31: Políticas de Importación en LDP

Usando una política de importación, Figura 31, prevenimos administrativamente la instauración de una selección, o incluso todas las uniones etiqueta-FEC en la tabla LFIB, pero sin embargo éstas se mantienen almacenadas en la tabla LIB.
La definición de qué es y cómo se estructura una política, fue explicada en el punto anterior, solo que en este caso el propósito es invalidar el comportamiento por defecto, modificándolo, aplicando en el router receptor la política dentro del protocolo LDP.

2.6.7 Retirada de etiquetas y Mensajes de Liberación.

Un router LDP lanza un mensaje de "Retirada de etiqueta" para dar la instrucción a sus *peers* de que han de retirar una etiqueta que se distribuyó previamente. Este hecho puede deberse a diversas razones, tanto administrativas como por casos de fallo.
Ante un mensaje de retirada de etiqueta, el router receptor generará un mensaje de "Liberación" que hace las veces de asentimiento o "*acknowledgment*".

Figura 32: Mensajes de Retirada y Liberación de Etiquetas

2.6.8 Autenticación en LDP

Podemos habilitar la autenticación dentro del contexto de LDP en el router, para evitar ataques contra las sesiones LDP que establecemos vía TCP.
La forma en que la autenticación MD5 (*Message Digest 5*) protege contra estos ataques es añadiendo una firma, también conocida como MD5 digest, a todos los segmentos TCP. La contraseña MD5 configurada se usa para calcular esta firma única para cada segmento TCP, y ésta nunca se transmite en texto plano hacia el otro extremo. El receptor, por su parte, utilizará igualmente la contraseña configurada para verificar la firma MD5, descartando el segmento TCP recibido si la verificación muestra un fallo.
Aunque en el momento de la configuración puede incluirse la contraseña en forma de hash o texto plano, los routers de servicio de Alcatel-Lucent no mostrarán nunca en sus salidas por pantalla la clave en texto plano, sino en modo hash, por razones obvias de seguridad.

2.6.9 LDP *Fast Re-Route*

Normalmente un router no debe de decidir de forma unilateral la forma en que reenvía los paquetes por sus interfaces, sino que ha de ser consecuente con las decisiones derivadas del uso de un protocolo de enrutamiento. De este modo, y basándose en los cálculos de algoritmos como el SPF (Dijkstra), usado en los IGP, OSPF y IS-IS, se pueden evitar bucles de enrutamiento.

Por tanto, cuando existe un cambio en la topología de la red, todo enrutador ha de ser informado del mismo, para actuar en consecuencia y establecer los caminos que los paquetes deberán tomar a partir de entonces. Este proceso durante el cual los routers intercambian y actualizan sus tablas para el reenvío óptimo de los paquetes, es conocido como re-convergencia y puede tardar más o menos en función del protocolo de enrutamiento.

A pesar de todo esto, existe la posibilidad de que los enrutadores calculen más de un camino a un destino, esto es, una ruta alternativa. Si el cálculo de esta ruta da como resultado un camino elegible que pueda usarse incluso sin avisar al resto de encaminadores en caso de fallo, puesto que carece de bucles, entonces, esto es a lo que denominamos *Loop-free alternate* (Alternativa Libre de Bucles) o LFA. Si un enrutador es capaz de calcular una ruta de este tipo, en caso de fallo del enlace principal que se está utilizando, el *router* podría decidir conmutar y usar el camino alternativo directamente, evitando impactar en el servicio debido a los tiempos de re-convergencia.

LDP puede hacer uso de estos caminos alternativos, si se configura para ello. En este caso si LDP utiliza esta funcionalidad derivada del propio protocolo de enrutamiento, es a lo que llamaremos LDP *Fast Re-Route* (Re-enrutamiento Rápido).

2.7 Túneles de Servicio

Como ya explicamos en el punto introductorio acerca de IP/MPLS, las redes que hacen uso de esta tecnología tienen como fin soportar diferentes tipos de servicios y aplicaciones. Dentro de una red de proveedor de servicios, una de las aplicaciones por excelencia para las que se requieren este tipo de redes MPLS es la de los servicios VPN (Redes privadas virtuales). Estos servicios brindan la oportunidad a las corporaciones (clientes potenciales del ISP) de interconectar sus emplazamientos (sedes) usando para ello la infraestructura común del proveedor de servicios. Desde el punto de vista del cliente, la red está "trabajando" únicamente en su beneficio, es decir, ellos perciben que la red está "dedicada" para ellos. Esta es una de las características de las redes IP/MPLS. Además el cliente disfruta de los beneficios de seguridad, privacidad, alta disponibilidad, fiabilidad y eficiencia. El hecho de establecer diferentes instancias de servicios en los "*Services Routers*" para cada cliente proporciona aislamiento entre el tráfico de éstos. Las instancias que pertenecen al mismo cliente se interconectan de manera virtual usando los denominados túneles de servicio, proporcionando interconexión de emplazamientos.

Los túneles de servicio “tunelizan”, valga la redundancia, el tráfico de los servicios VPN de un extremo a otro de la red (de PE a PE). El concepto tunelizar hace referencia siempre a transmitir información extremo a extremo, sin la necesidad de que haya una interpretación intermedia de la información que se transporta. Para poder establecer estos túneles de servicio extremo-extremo, necesitamos obviamente los túneles de transporte, previamente establecidos. Estos túneles de transporte son los que internamente llevan los túneles de servicio, lo cual ayuda en la escalabilidad, puesto que un túnel de transporte puede llevar varios túneles de servicio, véase el ejemplo de la Figura 33. Además proporcionan transparencia, puesto que los *routers* intermedios de la red MPLS, los Ps, sólo interpretarán la etiqueta que conforma el túnel de transporte.

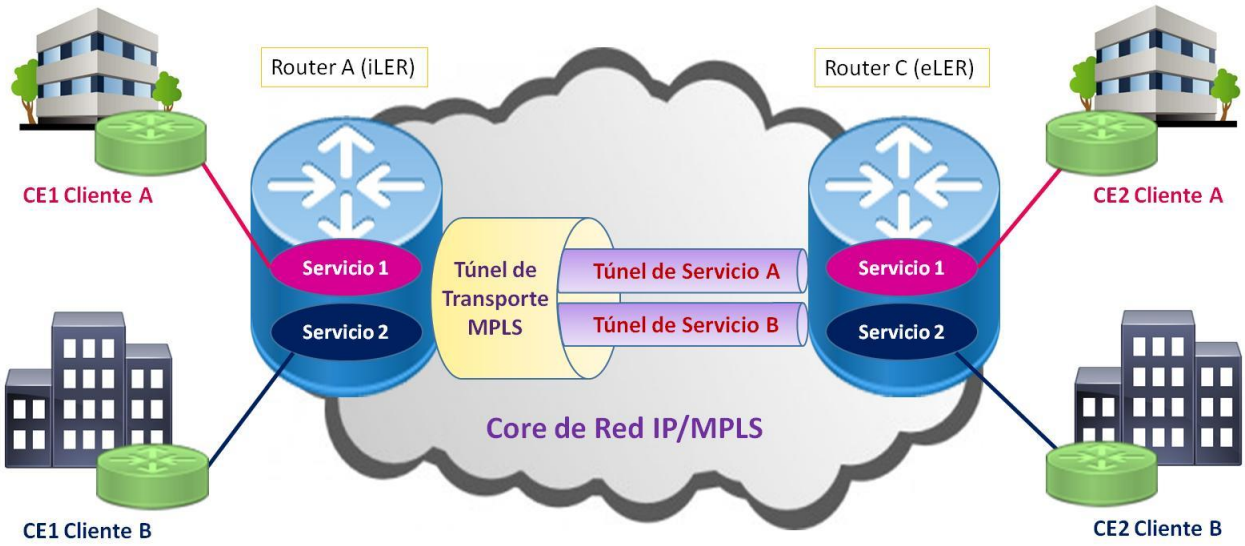


Figura 33: Túneles de Transporte y Servicio

Como consecuencia de lo descrito anteriormente, puede inferirse que estos servicios VPN que usan la red IP/MPLS implementan una pila de etiquetas. En este caso particular, la pila consta de un doble etiquetamiento. La etiqueta externa definirá cual es el túnel de transporte (salto a salto), mientras que la interna definirá el túnel de servicio (extremo a extremo). Destacar que los routers intermedios del *Backbone* (LSR), encargados de intercambiar las etiquetas, sólo procesan la etiqueta externa, necesaria para identificar el túnel de transporte, ya que la interna es insertada en el enrutador de ingreso y es usada por el enrutador de egreso para seleccionar la instancia de servicio (VPN) a la que debe dirigirse el tráfico que entra desde el núcleo. Este apilamiento de etiquetas permite al PE agregar el tráfico de varios clientes (VPNs distintas) en un solo túnel de transporte MPLS si es necesario.

Como se ha mencionado, las etiquetas de servicio se utilizan para “encapsular” e identificar el tráfico que pertenece a un servicio particular de cliente, añadiéndose a éste antes de insertar las etiquetas de transporte. En ocasiones a estas Etiquetas de Servicio (*Service Labels*) también se las conoce como VC Labels (*Virtual Circuit Labels*). Pero, ¿cómo indican los enrutadores de borde (PEs) las etiquetas de utilizaran para identificar

un determinado servicio? Esta pregunta nos lleva a definir los dos protocolos que utilizaremos para señalizar las etiquetas de servicio, dependiendo del tipo de servicio en sí:

- Las etiquetas de servicio para servicios VPWS o VPLS, esto es, servicios VPN de nivel 2, se señalizan usando T-LDP.
- Mientras, por su parte, los servicios VPN de nivel 3 como las VPRN, se señalizarán usando MP-BGP.

Durante los siguientes puntos entraremos en detalle acerca de estos dos métodos para señalizar etiquetas de servicio.

2.7.1 *Targeted* LDP (T-LDP)

Los Router de Servicio de Alcatel-Lucent, usan dos versiones del protocolo LDP, el *Link* LDP y el *Targeted* LDP (T-LDP). Acabamos de ver cuál es el funcionamiento del *Link* LDP, usado para el establecimiento de los túneles de transporte. Adicionalmente, en estos apartados se explicará y desarrollará el funcionamiento de T-LDP usado para señalizar las etiquetas de servicio y establecer los túneles de servicios para VPNs de capa 2 (capa de enlace) como VPLS o VLLs.

2.7.1.1 Sesiones TLDP

Acabamos de decir que tanto las sesiones “Link LDP” como las de “T-LDP” tienen propósitos distintos. Link LDP como se explicó forma adyacencias entre los *peers* directamente conectados. Mientas que T-LDP por el contrario, podrá formar adyacencias entre *peers* que no estén directamente conectados, esto es, habiendo elementos de por medio, véase uno o más LSRs. Esto tiene su justificación en el hecho de que los servicios se configuran en los PEs, por definición, equipos de frontera dentro de la IP/MPLS.

Resumiendo, T-LDP señaliza las etiquetas asociadas a servicios y no las asociadas a transporte como Link LDP.

Es por ello que podríamos utilizar T-LDP configurándolo en las propias interfaces, sin habilitar LDP. Los servicios VPN pueden por consiguiente configurarse para usar otros protocolos basados en túneles de transporte, como el mencionado RSVP-TE.

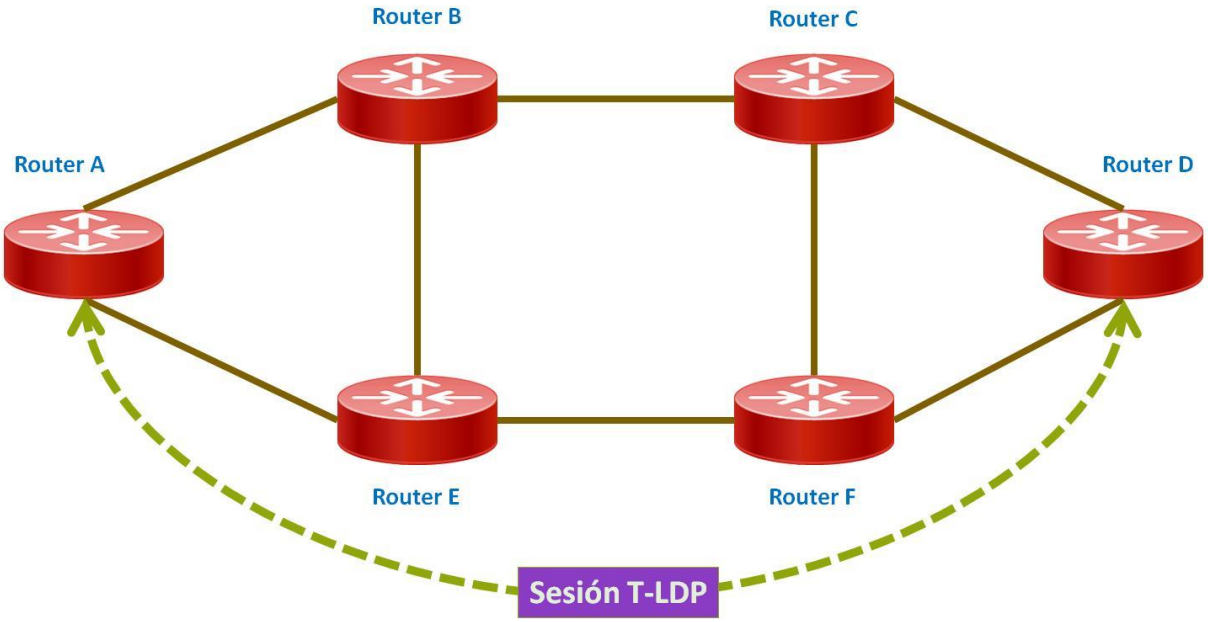


Figura 34: Establecimiento de sesiones T-LDP

NOTA: Aunque no es un ejercicio habitual dentro de las redes de proveedores de servicios, por su compleja administración y su falta de escalabilidad, podríamos configurar manualmente las etiquetas que conformaran los túneles de transporte, así como las etiquetas asociadas a los servicios.

2.7.1.2 Funcionamiento y operación T-LDP

El funcionamiento y operación de T-LDP es muy similar al descrito en el apartado del Link-LDP, usando mensajes de Hello, Init y Keep-alive. La principal diferencia radica en que los mensajes de Hello, intercambiados para establecer la adyacencia y posteriormente con fines de mantenerla, no se envían a una dirección de multicast sino a una dirección unicast UDP, esta es, la *System IP Address* del *peer*, el cual puede estar emplazado varios saltos más allá.
Los mensajes de Init siguen usándose para establecer la sesión, y los Keep-alive continúan enviándose periódicamente tras haberse establecido la sesión.

Igualmente, toda la información acerca de los parámetros *hello timeout* & *factor* y los *keep-alive timeout* & *factor* también aplican a la configuración de T-LDP.

2.7.2 *Multiprotocol - Border Gateway Protocol* (MP-BGP)

Aunque ya definimos qué es una VPRN en el punto 2.3.3, antes de desarrollar el funcionamiento y operación con MP-BGP, conviene introducir algunos conceptos sobre este servicio, que nos ayudarán a comprender mejor el porqué de su uso en el proceso de distribución de etiquetas de servicio.

2.7.2.1 Virtual Routing and Forwarding (VRF)

Una VPRN es un servicio que permite a múltiples emplazamientos de cliente, comunicarse entre sí, de manera segura a nivel IP, usando para ello la infraestructura de *Backbone* MPLS, de un ISP. Una sola infraestructura de *Backbone*, puede permitir el despliegue de multitud de servicios de este tipo para diferentes clientes, aislando unos de otros.

Como ya se mencionó anteriormente, este aislamiento pasa por la creación de tablas de enrutamiento separadas para cada instancia VPN (servicio), a las cuales denominamos VRFs (*Virtual Routing and Forwarding*). Su implementación de basa en el RFC 4364 [Ref. 9] (anteriormente RFC 2547bis [Ref. 10]).

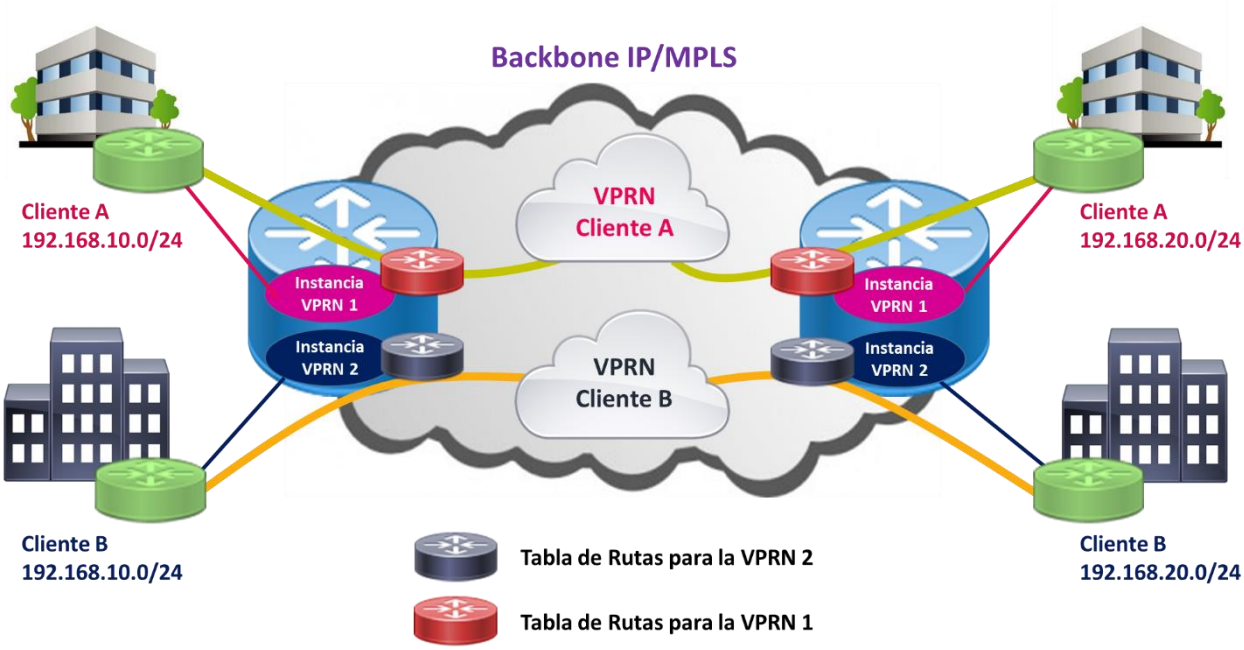


Figura 35: Esquema de un servicio VPRN

2.7.2.2 Route Distinguisher (RD)

Debido a la naturaleza privada de un servicio de VPN de capa 3 como lo es VPRN, el cliente puede decidir el direccionamiento IP a utilizar entre sus sedes, sin importar si éste se solapa con el usado por otros clientes. Para asegurar que las direcciones IP de cliente siguen siendo únicas cuando las distribuimos a través de nuestra red de Backbone, se utiliza un identificador de 8 bytes que antepondremos a los prefijos IPv4, al cual denominamos *Route Distinguisher* (RD), para conformar las llamadas direcciones VPN-IPv4.

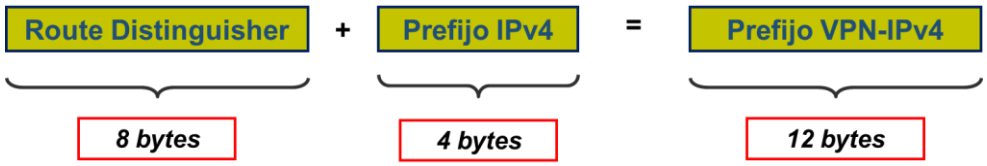


Figura 36: Prefijos VPN-IPv4

2.7.2.3 Route Target (RT)

Llegados a este punto, podemos deducir que un mismo grupo de PEs necesitarán intercambiar rutas de diferentes instancias de servicio del tipo VPRN. Pero para ayudar a mejorar la escalabilidad, los PEs sólo establecerán una sesión MP-BGP con cada PE que haya en la topología, para el intercambio del conjunto (familia) de prefijos VPN-IPv4. Ahora bien, si sólo se establece una sesión entre los enrutadores de la frontera, necesitamos de un mecanismo que nos ayude a determinar a qué VRF pertenece cada ruta que se intercambien los PEs.

A ese identificador que nos proporciona la membresía de una ruta a una VRF particular, lo denominamos *Route Target* (RT), y es el encargado de indicar al PE receptor de la ruta a qué tabla VRF está destinado dicho prefijo.

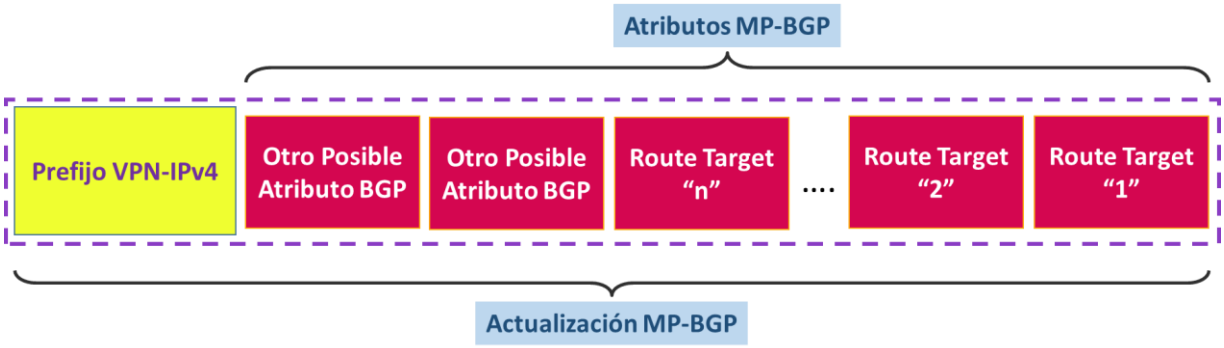


Figura 37: Componentes en un Anuncio (Actualización) MP-BGP

El identificador *Route Target* se añade como atributo a la actualización MP-BGP de cada ruta antes de compartirse con el resto de PEs, a través de la propia configuración de la VPRN de cliente, mediante el parámetro "vrf-target". De manera alternativa podríamos, en lugar de esto, definir una política de exportación para añadir el valor del Route Target (community attribute) a la ruta anunciada a los PEs remotos. Cuando un PE recibe esta ruta VPN-IPv4, añadirá por defecto el prefijo a la VRF que tenga asociado el mismo valor (por configuración) que el recibido (RT) en el anuncio de ruta. Este comportamiento también puede modificarse mediante la creación de una política de importación, que decidirá si añadir o no el prefijo a la VRF.

El identificador *Route Target* es uno de los atributos MP-BGP que pueden asociarse a una ruta, pero no el único. Una misma ruta puede tener asociados varios RTs. Esto ofrece versatilidad a la hora de conformar la arquitectura lógica de una VPRN. Si sumamos además una coherente administración de políticas de exportación e importación habremos conseguido el aislamiento (seguridad) que buscábamos para cada Red Privada de cliente.

A pesar de todo esto, el valor del RT suele coincidir a menudo con el valor designado para el RD, por seguir una consistencia en la provisión de los servicios. Sin embargo no se han de confundir ambos conceptos identificando uno con el otro, porque pueden no coincidir, ya que se usan para funcionalidades distintas.

2.7.2.3 Sesiones MP-BGP

Acabamos de mencionar que los enrutadores de frontera (PEs) únicamente establecerán una sesión del protocolo BGP entre sí para sus anuncios de rutas, usando las extensiones de MP-BGP, que no son más que un mecanismo para la distribución de información adicional de enrutamiento de las VPRNs, como son los prefijos VPN-IPv4, los "*extended community attributes*" (como el RT), o las Etiquetas de servicio VPN (VPN *Labels*), que se verán a continuación.

Nota: Como consecuencia tendremos un mallado completo de sesiones BGP entre los PEs de la solución. En proveedores de interconexión de redes y servicios (ISPs) muy grandes, en los que el número de equipos en la frontera es elevado, las sesiones se establecen contra unos equipos denominados Reflectores de Rutas (suelen provisionarse dos equipos), lo cual evita realizar un mallado de sesiones completo entre los PEs.

Se ha de subrayar que se han de establecer sesiones BGP separadas para cada familia (conjunto) de direcciones que necesiten intercambiar entre ellos. Cuando BGP se configura de esta forma, es cuando se le denomina MP-BGP (Multiprotocolo BGP). Se menciona esto ya que los anuncios de rutas para la familia de prefijos IPv4 estándar se llevan a cabo mediante el establecimiento de otra sesión BGP distinta.

Nótese que la familia o conjunto de direcciones VPN-IPv4 se usa sólo en el plano de control, cuando intercambiamos los mensajes de actualización de rutas en MP-BGP entre los routers de borde. Incluso los prefijos IPv4 anunciados procedentes de los equipos CE (*Customer Edge*) se guardan dentro de las VRFs sin el RD o el RT.
Ni siquiera el cliente es consciente de la existencia de las direcciones VPN-IP, ya que en el plano de datos todo el tráfico es transportado usando paquetes IPv4 estándar, encapsulados con las correspondientes etiquetas (transporte y servicio).

2.7.2.4 Etiquetas de Servicio – VPN Labels

Cuando el tráfico de cliente llega a través del *Backbone* IP/MPLS al enrutador PE de egreso, se ha de conocer cómo reenviar el paquete al destino correspondiente, y esto dependerá de a qué cliente pertenezca el mencionado tráfico. Este proceso de "demultiplexación" del tráfico procedente de las VPN puede realizarse gracias al uso de las VPN *labels* (Etiquetas de servicio).

Estas etiquetas de servicio se distribuyen mediante el protocolo MP-BGP, de ahí que lo consideremos un protocolo para la creación de túneles de servicio.
Como podemos deducir de lo dicho anteriormente, estas etiquetas no viajan solas en las actualizaciones de rutas del MP-BGP, sino que van siempre acompañadas de más información asociada a la propia ruta, como el atributo RT que se expuso en el apartado anterior (véase el ejemplo de la Figura 38).

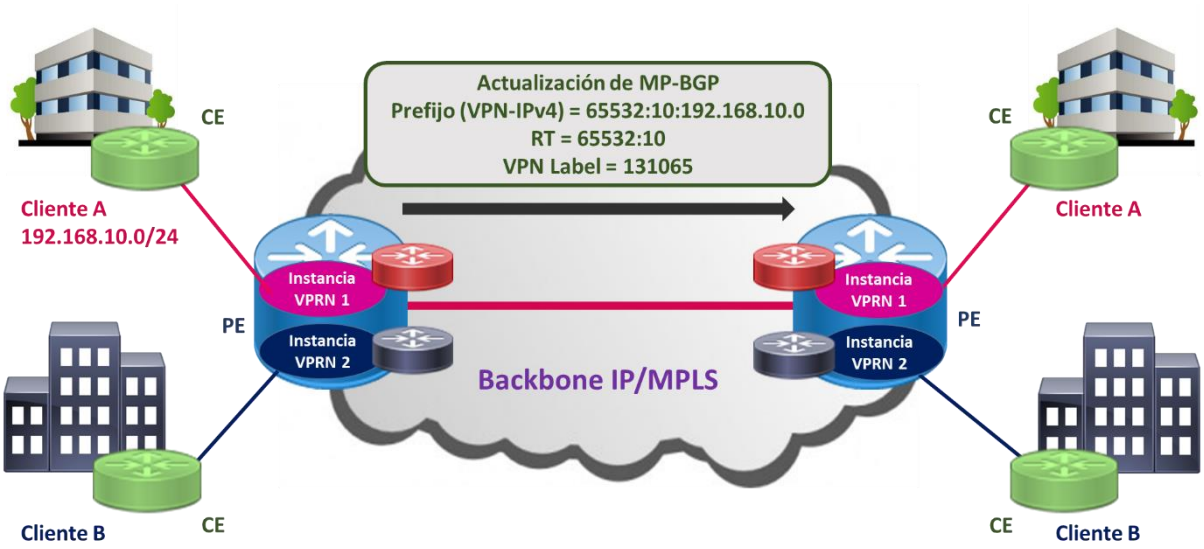


Figura 38: Envío de la VPN Label a través de MP-BG

La VPN *Label* que viaja con los paquetes de información, en el plano de datos, nos indicará qué VRF debe usarse para llevar a cabo la búsqueda del siguiente salto para el destino del paquete, o el propio siguiente salto, y así reenviar correctamente el tráfico.

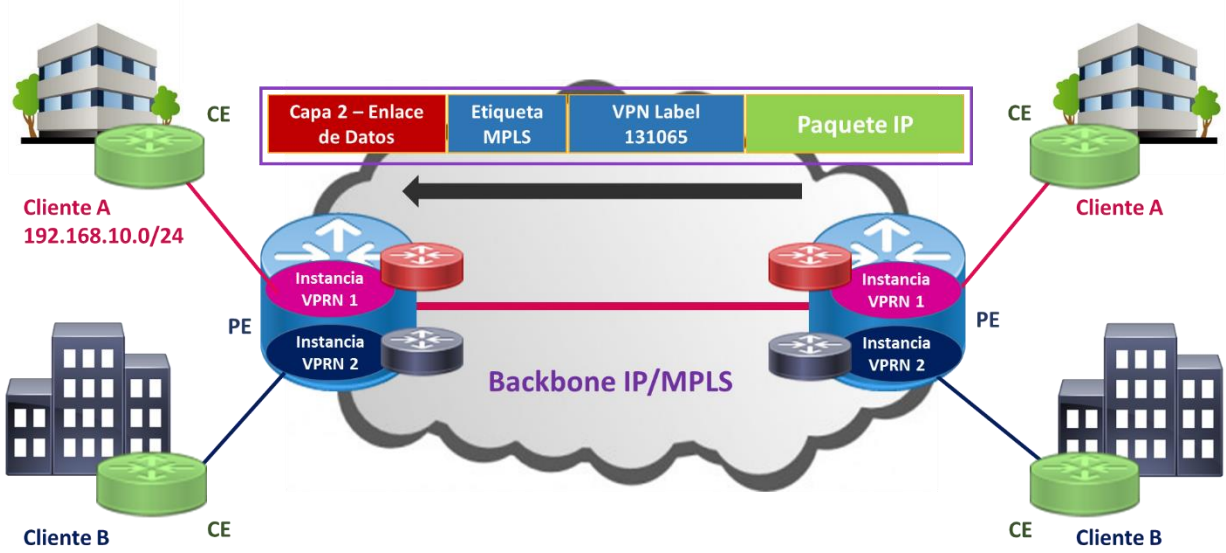


Figura 39: Uso de una VPN Label

2.7.2.5 Túneles de Transporte – Plano de Datos

Aunque no se ha mencionado anteriormente, cada PE involucrado en un servicio VPRN debe de tener establecido un túnel con el resto de PEs participantes en la misma VPRN, con el fin de transportar el tráfico de una localización de cliente a otra. Estos túneles se establecerán tras crearse la topología de enrutamiento, con ayuda del protocolo de encaminamiento IGP utilizado, y mediante LDP o RSVP-TE. Estos túneles no son más que LSPs de MPLS que usan los paquetes del tráfico de cliente para ser transportados por el *Backbone* de la red.

En general, no sólo dentro del servicio VPRN, ha de haber una asociación de estos túneles de transporte con los servicios. Esta asociación puede llevarse a cabo de diferentes formas. En el caso que nos ocupa, los equipos Alcatel-Lucent ofrecen varias posibilidades:

- Configurando los denominados SDPs (*Service Distribution Points*). Estas entidades necesitan en su definición un LSP a utilizar como medio de transporte para el plano de datos. Son unidireccionales, al igual que los LSPs que usan, y también pueden ser usados por varios servicios a la vez. Son la opción usada en servicios VPN de nivel 2.

  Cuando asociemos el SDP al servicio en cuestión, se debe indicar un VC-ID, que debe coincidir en ambos extremos (PEs) del SDP, puesto que la etiqueta VC *Label* (Etiqueta de servicio) que se negociará automáticamente mediante T-LDP, irá asociada al valor VC-ID elegido.

- En el caso de los servicios VPN de nivel 3, VPRNs, como el que estábamos viendo, y ya que la negociación de la etiqueta de servicio (VPN *Label*) se lleva a cabo a través de las sesiones de MP-BGP entre los PEs, podemos utilizar una opción denominada "*auto-bind*" en el momento de configuración de la instancia de servicio. Esta opción sólo está disponible para las VPRNs que tienen establecidas sesiones MP-BGP entre cada par de *routers* de la VPN, y tienen ya identificados a sus *peers*. Por consiguiente, el comando de auto-bind creará automáticamente los SDPs (incluyendo los LSPs negociados mediante LDP o RSVP-TE) contra todos los routers con los que exista una sesión MP-BGP para la familia de prefijos VPN.

Capítulo 3: Equipamiento y componentes de la solución

3.1 Alcatel-Lucent 7750 SR

Como ya se mencionó en la introducción, y por petición expresa del cliente, el despliegue de la red IP/MPLS se llevará a cabo con equipamiento Alcatel-Lucent. Más concretamente con dos modelos diferentes en cuanto a capacidades, pero iguales a la hora de configurar y trabajar con ellos. Estos son:

- 7750 SR – 12
- 7750 SR – 7

Figura 40: Equipamiento – 7750 Service Routers [Ref. 11]

Ambos chasis se encuentran dentro de la familia de productos 7750 SR de Alcatel-Lucent y, como consecuencia, ambos están diseñados para proporcionar alto rendimiento y alta disponibilidad en escenarios exigentes en cuanto a enrutamiento y gestión de servicios se refiere. La numeración que acompaña a cada uno de los equipos hace referencia a la cantidad de ranuras (slots) disponibles para la inserción de tarjetería, aunque en estos modelos dos de los "*slots*" para tarjetas se destinan a alojar las tarjetas SF/CPM (*Switch Fabric/Control Processor Module*) (redundancia 1+1 para asegurar la alta disponibilidad), las cuales proporcionan la potencia de procesamiento y constituyen el plano de control y de conmutación de los equipos (soportan hasta 2 Tbits/s en half-dúplex). Se detallarán más aspectos acerca de estas tarjetas a continuación (información directamente recogida del fabricante en sus *DataSheets*). Ambos modelos poseen doble fuente de alimentación.

Una característica destacada es la orientación a servicios que tienen estos enrutadores, los cuales están diseñados para facilitar la gestión, administración, mantenimiento y operación de servicios.

Tanto el 7750 SR – 12 como el 7750 SR – 7 hacen uso del nuevo chip procesador de Alcatel-Lucent FP3 (*Flex Path 3*) de menor tamaño, menor consumo y lo que es más destacable, mayor velocidad. Con sus 288 núcleos procesadores tipo RISC es capaz por ejemplo de procesar paquetes a 400 Gigabits por segundo, proporcionar hasta 5 millones de entradas en su tabla de rutas, o gestionar 32 mil interfaces de capa 3. En cuanto a los servicios, permite la creación de hasta 32 mil instancias VPRN, 96 mil instancias VPLS (pueden almacenarse 4 millones de MACs en total) o gestionar 256 mil terminaciones de VLLs.

Otra característica a destacar de estos equipos es su modularidad y amplia gama de tarjetería. Algunas de estas tarjetas, que usaremos en la implementación, se detallan a continuación con ayuda de las *DataSheet* del fabricante.

3.2 Hardware y tarjetas soportadas

Aunque no detallaremos todos los medios soportados por los equipos, si se explicarán algunos de los módulos insertables (tarjetas) que cabe la pena destacar debido a su uso en la implementación en este proyecto. Todas las tarjetas mencionadas a continuación pueden alojarse tanto en el chasis 7750 SR - 7 como en el chasis 7750 - 12:

- Las tarjetas SF/CPM (*Switch Fabric/Control Processor Module*) son módulos insertables que ocupan un *slot* completo dentro del chasis. Se encarga del plano del datos (SF), haciendo las veces de matriz de conmutación de altas prestaciones y del plano de control (CPM), para la gestión de los protocolos y servicios que maneja el enrutador (funcionalidades divididas, de ahí su nombre). Como ya se mencionó anteriormente, normalmente se montan dos tarjetas en redundancia 1+1 activa-activa, en reparto de carga. Son reemplazables en caliente, lo cual ofrece un punto extra de continuidad en la prestación de servicios (Figura 41, tarjetas A y B).
- Los módulos IOM (Input/Output Modules) son el punto de unión con las interfaces físicas. Contienen dos procesadores de tráfico programables soportando ambas ranuras la inserción de una MDA (*Media Dependent Adapters*) o una ISA (*Integrated Service Adapters*). Cada tarjeta posee una unidad central de procesamiento para gestionar el reenvío de los procesadores de tráfico. Es por ello que aquí se alojan las bases de datos (tablas) de reenvío para direcciones IP y MAC, además de las listas de control de acceso o la configuración para los mecanismos de calidad de servicio. De nuevo, estos módulos son intercambiable en caliente, (Figura 41, tarjetas 1-9).
- La función principal de las tarjetas MDAs es la de hacer de terminación física de diversas tecnologías, tanto ópticas como eléctricas, como pueden ser Ethernet, ATM, TDM, POS (*Packet over Sonet*/SDH), CES (*Circuit Emulation Services*), etc. Las MDAs direccionan el tráfico de ingreso hacia la IOM para su procesamiento, y en egreso lo hacen hacia la interfaz apropiada en el formato adecuado. Al igual que las propias IOM donde se alojan, son intercambiable en caliente.

- Las interfaces SFP (*Small Form-factor Pluggable*) son módulos que hacen las veces de transceptores ópticos de pequeño tamaño (los hay en diversos formatos), insertables dentro de las MDAs (aunque no todas los soportan).
- Otros de los módulos insertables en un *slot* completo, son los denominados IMM (*Integrated Media Modules*), muy parecidos a las IOM pero uniendo el procesamiento y las interfaces físicas en una única tarjeta.
- Las tarjetas ISA insertables en los módulos IOM son un tipo especial de MDA. No poseen puertos físicos, pero son tarjetas que proporcionan recursos y procesamiento especializado. Se utilizan para el establecimiento y control de túneles IPSec, Servicios de Video, NAT (Traducción de Direccionamiento de Red), etc.

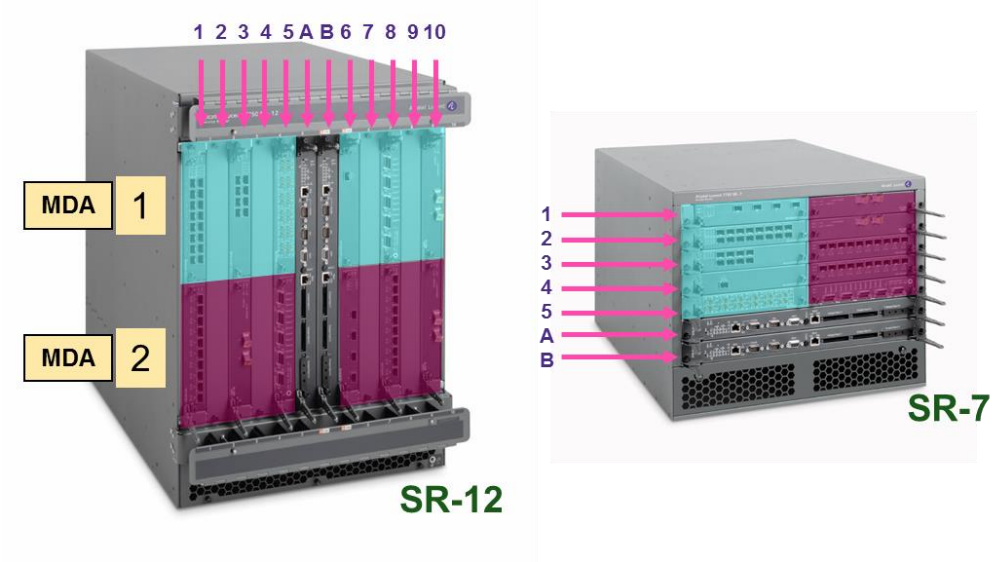


Figura 41: Equipamiento – Módulos y tarjetas [Ref 12]

Las siguientes tablas resumen la información acerca del hardware (características sacadas directamente de las DataSheet del fabricante):

	7750 SR-c4	7750 SR-c12	7750 SR-7	7750 SR-12	7750 SR-12e
System throughput	• Integrated 90 Gb/s • Switch fabric (half duplex)	• Redundant CFM-XP switch fabric • 90 Gb/s (half duplex) with 1+1 redundancy	• Switching capacity: 2 Tb/s (half duplex, redundant) • Per-slot throughput: 200 Gb/s (full duplex, redundant)	• Switching capacity: 4 Tb/s (half duplex, redundant) • Per-slot throughput: 200 Gb/s (full duplex, redundant)	• Switching capacity: 9.6 Tb/s (half duplex, non-redundant) or 7.2 Tb/s (half duplex, redundant) • Per-slot throughput: 400 Gb/s (full duplex, redundant)
Built-in network interfaces	• 2 x 10GBASE (LAN/WAN PHY) XFP • 10/100BASE Management Ethernet RJ-45	• 10/100BASE Management Ethernet RJ-45	–	–	–
Number of MDAs per chassis	2	6	10	20	18
Number of CMAs per chassis	4	8 (plus 2 MDAs)	–	–	–
Number of IOMs/IMMs/ISMs per chassis	–	–	5	10	9
Common equipment redundancy	• Power entry modules (PEMs), fans	• CFM-XP, PEMs, fans	• SFM5-7, CPM5, SF/CPM, PEMs, fans	• SFM5-12, CPM5, SF/CPM, PEMs, fans	• SFM5-12e, CPM5, SF/CPM, Mini-SFM, advanced power equalizers (APEQs), fans

Figura 42: Especificaciones Técnicas para el portfolio Alcatel-Lucent 7750 SR [Ref.13]

IMM TYPE	PORTS PER IMM	CONNECTOR TYPE	SR-7	SR-12	SR-12e
100GBASE	4	CXP and CFP4	–	–	√
100GBASE	1, 2	CFP	√	√	√
100GBASE/10GBASE	1/10	CFP/SFP+	√	√	√
100GBASE + 7x50 ISA2	1	CFP	√	√	√
100GBASE IMM (DWDM tunable optics)	1	LC	√	√	√
40GBASE	3, 6	QSFP+	√	√	– / √
40GBASE/100/100BASE	3/20	QSFP+/SFP	√	√	√
10GBASE	40	SFP+	–	–	√
10GBASE/100/100BASE	10/20	SFP+/SFP	√	√	√
10GBASE + 7x50 ISA2	10	SFP+	√	√	√
10GBASE	12, 20	SFP+	√	√	√
10GBASE	5, 8	XFP	√	√	√ / –
10/100/1000BASE	160/80	CSFP/SFP	√	√	√
10/100/1000BASE	48	SFP	√	√	√
10/100/1000BASE-TX	48	RJ-45	√	√	√

Figura 43: Tipos de IMM soportadas por cada clase de chassis [Ref. 14]

	7750 SR-c4	7750 SR-c12	7750 SR-7	7750 SR-12	7750 SR-12e
Hot-swappable modules	• MCM-XPs, MDAs, ISAs, CMAs, PEMs, fans	• CFM-XP, MCM-XPs, MDAs, ISAs, CMAs, PEMs, fans	• SFM5-7, CPM5, SF/CPM, IOMs, MDAs, IMMs, ISMs, ISAs, VSMs, EFTs	• SFM5-12, CPM5, SF/CPM, IOMs, IMMs, ISMs, MDAs, ISAs, PEMs, VSMs, EFTs	• SFM5-12e, CPM5, SFM/CPM-12e, Mini-SFM-12e, IOMs, MDAs, IMMs, ISMs, ISAs, VSMs, APEQs, EFTs
Dimensions**	• Height: 13.8 cm (5.4 in), 3 RU • Width: 44.5 cm (17.5 in) • Depth: 47 cm (18.5 in)	• Height: 22.2 cm (8.8 in), 5 RU • Width: 44.5 cm (17.5 in) • Depth (with cable management): 60 cm (23.6 in)	• Height: 35.6 cm (14 in), 8 RU • Width: 44.5 cm (17.5 in) • Depth: 64.8 cm (25.5 in)	• Height: 62.2 cm (24.5 in), 14 RU • Width: 44.5 cm (17.5 in) • Depth (without cable management): 64.5 cm (25.4 in) • Depth (with cable management): 76.5 cm (30.1 in)	• Height: 97.8 cm (38.5 in), 22 RU • Width: 44.5 cm (17.5 in) • Depth: 76.2 cm (30 in)
Weight**	• Empty: 13.6 kg (30 lb) • Loaded: 21.8 kg (48 lb)	• Empty: 16.5 kg (36.4 lb) • Loaded: 45.4 kg (100 lb)	• Empty: 41 kg (90.4 lb) chassis weight with factory installed fan tray and air filter • Loaded: 70.5 kg (155.4 lb)	• Empty: 56.4 kg (124.3 lb) • Loaded: 155.7 kg (343.3 lb)	• Empty: 79.4 kg (175 lb) • Loaded: 249.5 kg (550 lb)
Power	DC power: • Voltage: -40 V DC to -60 V DC • Current: 9 A to 14 A • 1+1 redundancy AC power: • Input voltage: 110 V AC to 240 V AC • Current: 2.3 A to 5.5 A • 50 Hz to 60 Hz	DC power: • Voltage: -40 V DC to -60 V DC • Current: 22 A to 28 A • 1+1 redundancy AC power: • Input voltage: 220 V AC to 240 V AC • Current: 6 A • 50 Hz to 60 Hz	DC power: • Voltage: -40 V DC to -72 V DC • Current: 52 A to 93 A • 1+1 redundancy External AC power (option): • Input voltage: 200 V AC to 240 V AC • Output voltage: 42 V DC to 56 V DC • Current: 50 A	DC power: • Voltage: -40 V DC to -72 V DC • Current: 90 A to 162 A • 1+1 redundancy External AC power (option): • Input voltage: 200 V AC to 240 V AC • Output voltage: 42 V DC to 56 V DC • Current: 50 A	DC power: • Voltage: -40 V DC to -72 V DC • Current: 60 A max • 4+1 redundancy External AC power (option): • Input voltage: 200 V AC to 240 V AC • Output voltage: 42 V DC to 56 V DC • Current: 50 A
Cooling	Side-to-side air flow	Side-to-side air flow	Side-to-back air flow	Front-to-back air flow	Front-to-back air flow

Figura 44: (Cont.) Especificaciones Técnicas para el portfolio Alcatel-Lucent 7750 SR [Ref. 15]

MDA TYPE	PORTS PER MDA	CONNECTOR TYPE	SR-c4	SR-c12	SR-7	SR-12	SR-12e
Ethernet MDA-e							
10GBASE	10	SFP+	–	–	√	√	√
100GBASE	1	CFP2	–	–	√	√	√
Ethernet MDA-XP							
1000BASE	10/12/20	SFP	√ / - / √	√ / - / √	√	√	√
10/100/1000BASE-TX	20	RJ-45	√	√	√	√	√
10/100/1000BASE-TX	48	6 x mini RJ-21	–	–	√	√	√
10GBASE/1000BASE (LAN/WAN PHY)	2+12	XFP/SFP	–	–	√	√	√
10GBASE (LAN/WAN PHY)	1/2/4	XFP	√ / √ / -	√ / √ / -	√	√	√
High-Scale MDA							
1000BASE	10	SFP	–	–	√	√	√
10GBASE	1	XFP	–	–	√	√	√
SDH/SONET MDA-XP							
OC-192c/STM-64c	2	XFP	–	–	√	√	√
SDH/SONET MDA							
OC-3c/STM-1c/OC-12c/STM-4c (Multirate)	16	SFP	√	√	√	√	√
OC-48c/STM-16c	4	SFP	√	√	√	√	√
Any Service Any Port (ASAP) MDA							
Channelized DS3/E3 ASAP	4/12	1.0/2.3 connectors	√	√*	√	√	√
Channelized OC-3/STM-1 ASAP	4	SFP	√	√*	√	√	√
Channelized OC-12/STM-4 ASAP	1	SFP	√	√*	√	√	√
Asynchronous Transfer Mode (ATM) MDA							
ATM OC-3c/STM-1c/OC-12c/STM-4c (Multirate)	4	SFP	√	√*	√	√	√
ATM OC-3c/STM-1c	16	SFP	–	–	√	√	√
Other							
Versatile Service Module-XP	N/A	N/A	–	–	√	√	√

* A limit of two MDAs of type ASAP or ATM is supported in the 7750 SR-c12.

Figura 45: Tipos de MDAs soportadas por cada clase de chasis [Ref. 16]

Como es obvio, en esta fase del proyecto todavía no se dimensionarán capacidades debido a que aún no se tiene constancia de los clientes operativos, sino únicamente de los potenciales, por lo que no se utilizarán los recursos totales de los equipos. Por ello, en el despliegue se hará uso únicamente de la tarjetería necesaria para la interconexión de los elementos de red y de los equipos necesarios para desplegar el escenario que servirá de base para la futura prestación de servicios.

Más adelante, en el capítulo concerniente al diseño, despliegue y configuración de la solución, así como en el relacionado con el presupuesto del proyecto, se detallará la cantidad de equipamiento y tarjetería de los cuales se ha hecho uso.

Capítulo 4: Diseño, Implementación y Configuración de la solución

4.1 Diseño

Para el diseño de la solución hemos de tener en cuenta obviamente los requisitos exigidos por el cliente. Estos requisitos se basan principalmente en el reaprovechamiento del espacio que posee en sus emplazamientos distribuidos sobre la Comunidad de Madrid, región en la cual se desarrollaba su principal actividad como proveedor de acceso, y donde se dispondrán los POPs (*Points of Presence* – Puntos de Presencia) que servirán de interconexión entre los futuros usuarios y la red de proveedor a desplegar.

Estos POPs se encuentran situados en los extremos norte y sur de la ciudad de Madrid, uniéndose entre sí por un anillo urbano de fibra formado por canalizaciones por las que se transportan cables de hasta 256 fibras monomodo. Como ya se dijo el cliente se basará en esta infraestructura ya desplegada para la interconexión de los equipos de *backbone* de la red IP/MPLS.

Dado que la red de acceso ya está desplegada, el cliente ya posee equipos para la terminación de los diversos accesos (ATM, Frame Relay, Líneas conmutadas, Ethernet, Líneas dedicadas, etc.) en los POP.

Algunos de los equipos que servían de elementos de terminación (p.ej. RAS, BAS) o routers para terminación de las líneas dedicadas, podrán desaparecer trasladando sus funcionalidades a tarjetería dentro de los routers de borde (PEs) de la red de *backbone* IP/MPLS. Por tanto nuestros esfuerzos se centran ahora en el diseño del nivel de concentración/agregación y del nivel de *backbone*/núcleo, en cada POP.

Cuando hablamos de una "estructura jerárquica" sobre redes complejas, como lo es la subdivisión en red de acceso, concentración/agregación y backbone/núcleo de un ISP, no estamos más que atribuyendo un cometido específico a los equipos de red que componen la estructura global.

En nuestro caso particular, hacemos la distinción entre routers agregadores /concentradores y routers de backbone/núcleo (los de acceso no entran dentro de los objetivos de este proyecto). Los primeros se encargarán de agregar los accesos de los clientes y los segundos de proporcionar un transporte eficaz y rápido entre aquellos elementos que conformen el *backbone*. Obviamente las características que los definen, vienen dadas por la propia función del encaminador. Mientras los routers de agregación/concentración tienen como objetivo brindar un gran número de puertos con velocidades "relativamente" bajas de cara a cliente, los enrutadores de backbone/núcleo tienen como fin el alcanzar tasas de reenvío muy elevadas en las interfaces de interconexión dentro de la red del proveedor de servicios.

Conforme se incrementan las capacidades de cómputo de los actuales dispositivos de red, y como ya se mencionó, el hardware se especializa (ASIC - *Application-Specific Integrated Circuits*), las funcionalidades de los enrutadores tienden a mezclarse, por lo

que en ocasiones nos encontramos que un mismo modelo de enrutador puede hacer las veces de concentrador o de *router* de *backbone* sin más que unos cambios en tarjetería.

Aunque esta separación es cada vez más borrosa, si bien es cierto que nos sirve al menos a nivel lógico, para comprender la arquitectura de la red. Por otro lado, si lo pensamos bien, si los *routers* del núcleo desaparecieran habría de existir una red mallada completa entre los equipos de frontera.

Hablando en términos de VPNs, los *routers* concentradores pasan a denominarse PEs y los *routers* de backbone se denominan Ps.

A pesar de que ya se han establecido algunas de las características principales de las redes de agregación y *backbone* a continuación se describen algunos puntos clave, que se tuvieron en cuenta para llevar a cabo el diseño:

- En una red de agregación o concentración de accesos se necesita una alta densidad de puertos y ancho de banda suficiente para satisfacer la demanda de tráfico de diferentes clases (voz, video, datos) y de diferentes clientes, sin olvidar el potencial aumento futuro del negocio. Idealmente han de usarse equipos ágiles, capaces de concentrar gran volumen de tráfico y que, gracias a su software, posibiliten la venta de valor añadido al negocio, como la creación de VPNs, diferenciación del tráfico en diversas calidades de servicio, multicast, etc. No por ello hemos de olvidar que han de tener excelentes prestaciones y versatilidad, trabajando con protocolos de enrutamiento como RIPv2, OSPF, ISIS, BGP, etc.
- Por otro lado la red del núcleo tiene como principal objetivo mover el tráfico agregado de los clientes, procedente de los equipos de borde, a altas velocidades. Por esta razón, los nodos dentro del *backbone* no precisan de funcionalidades complejas sino que se centran en el reenvío a gran velocidad de mucho volumen de tráfico. El número de interfaces tampoco es elevado en estos equipos, aunque sí son interfaces de alta velocidad. Éstas serán las encargadas de interconectar los POPs de la red, y de dar conectividad, si es necesaria, con otros proveedores.
- Aunque existen muchos modelos en el diseño de este tipo de redes de *backbone* para los ISPs, todos buscan, como es evidente, reducir el retardo medio en el reenvío de los paquetes, sin dejar de lado la respuesta ante fallos. El retardo medio hoy en día es esencial, (vivimos en una red globalizada que utiliza continuamente la interacción multimedia y en tiempo real), y valores elevados de retardo pueden impedir una interacción fluida. Para ayudar a mejorar este hecho, se ha tenido en cuenta que el número de saltos dentro de la red del núcleo de un ISP no suele superar el valor 3 y que la capacidad de los enlaces entre nodos, así como una topología redundante (en caso de imprevistos), han de ser cruciales si deseamos una red estable, escalable y que perdure en el tiempo.

Aunque en este proyecto no se tenga en cuenta por estar fuera de su alcance, es importante mencionar que en entornos reales de proveedor, los POP pueden contener los denominados CPDs (Centro de Procesamiento de Datos), aprovechando el

emplazamiento e instalaciones acondicionadas a tal efecto. Esto es así en gran medida por ahorro de costos, alquiler (si lo hubiere), energía, ventilación, acondicionamiento, etc. En ellos se alojan servidores DNS, Servidores de Autenticación (RADIUS, DIAMETER, etc.), máquinas de gestión, visualización, monitorización… Todos ellos protegidos con firewalls, que tratan de evitar las intrusiones y fugas de información.

Teniendo en cuenta las consideraciones anteriores, un esquema general sería el mostrado en la Figura 48:

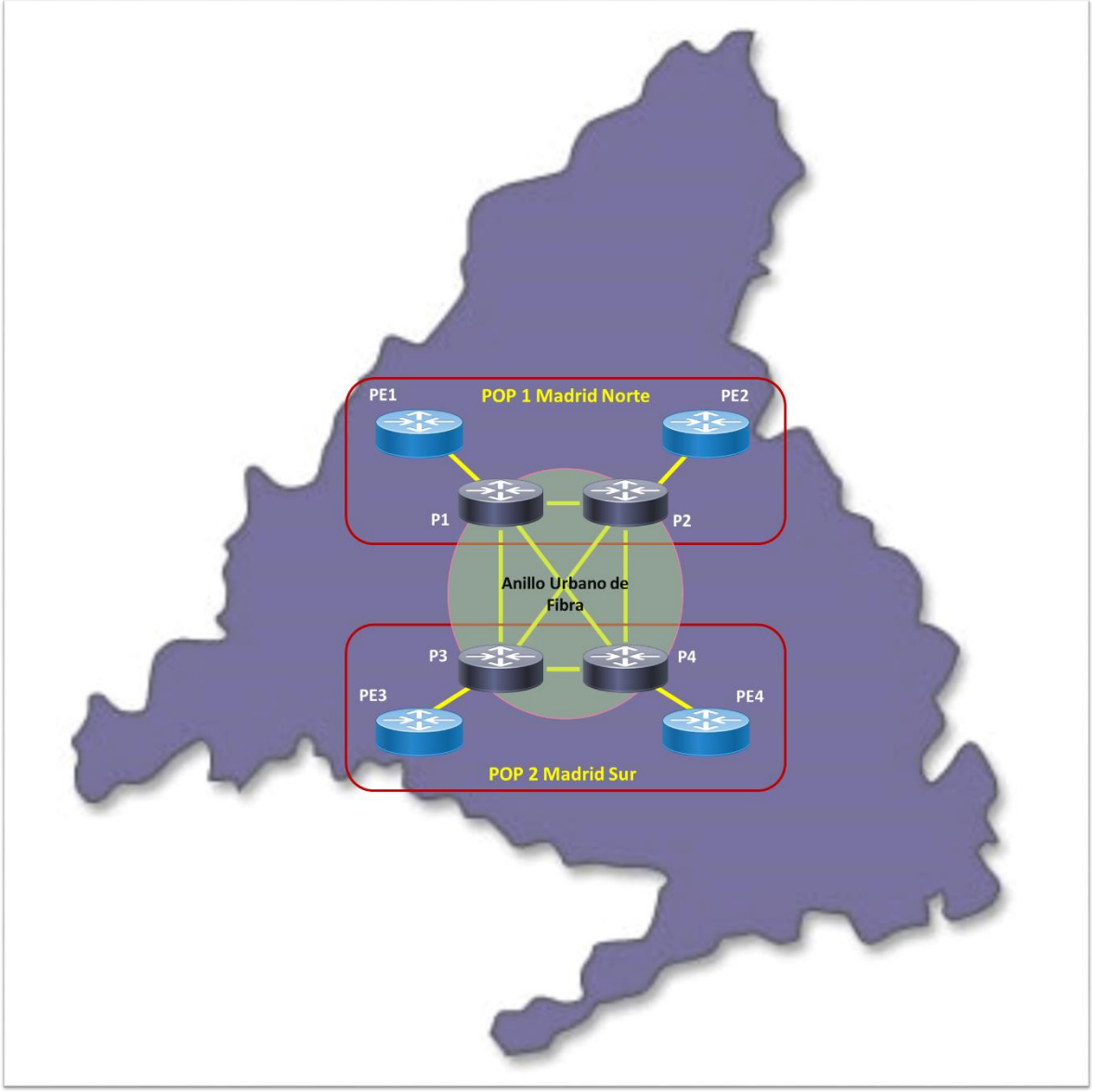


Figura 46: Esquema de diseño para el despliegue de la solución

Este diseño pone de manifiesto alguno de los aspectos importantes que recalcamos anteriormente, como que el número de saltos dentro del backbone no sea mayor de 3 o que los enlaces entre elementos del b*ackbone* estén redundado utilizando la infraestructura de fibra. Aunque no se muestre en la figura, los accesos de clientes

finales suelen estar redundados a diferentes PEs de frontera, por lo que la conectividad de los PEs a los Ps decidió no redundarse, entendiendo que el fallo de estos enlaces es menos probable, más rápido y más sencillo de solventar al no discurrir por vía pública y estando localizados en el propio POP ambos nodos.

4.2 Implementación

En esta fase de implementación del proyecto, y usando como referencia el diseño y equipamiento definido con anterioridad, se llevó a cabo un estudio con cliente para definir el despiece final de la solución, teniendo en cuenta el equipamiento del que ya se disponía en los POP para la interconexión de equipos, líneas futura de negocio y el crecimiento potencial en el número de clientes finales. Vistos estos factores, y teniendo en cuenta una estimación a medio plazo del retorno sobre la inversión, los elementos desplegados serán los siguientes:

Emplazamiento	Equipamiento	Descripción	Despiece (Tarjetas) por Equipo
POP 1 Madrid Norte	2 x (Alcatel-Lucent 7750 SR-12)	Equipos P de core de la red de backbone a modo de enrutadores de tránsito para el reenvío de tráfico.	• 4-port 100GE CXP IMM • 1-port 100GE CFP+10-port 10GE SFP+ • 2 x (4-port 10GBase MDA-XP [XFP]) • 8 x (1-port 10GBase MDA [DWDM tunable])
POP 1 Madrid Norte	2 x (Alcatel .Lucent 7750 SR-7)	Equipos PE de frontera de la red de backbone a modo de agregadores/disgregadores de tráfico de entrada/salida a la red.	• 160-port GE CSFP/SFP IMM • 2-port 100GE CXP IMM • 2 x (48-port 10/100/1000BASE-TX MDA-XP) • 2 x (2-port OC-192c/STM-64c MDA-XP) • 2 x (16-port ATM OC-3c/STM-1c)
POP 2 Madrid Sur	2 x (Alcatel-Lucent 7750 SR-12)	Equipos P de core de la red de backbone a modo de enrutadores de tránsito para el reenvío de tráfico.	• 4-port 100GE CXP IMM • 1-port 100GE CFP+10-port 10GE SFP+ • 2 x (4-port 10GBase MDA-XP [XFP]) • 8 x (1-port 10GBase MDA [DWDM tunable])
POP 2 Madrid Sur	2 x (Alcatel .Lucent 7750 SR-7)	equipos PE de frontera de la red de backbone a modo de agregadores/disgregadores de tráfico de entrada/salida a la red.	• 160-port GE CSFP/SFP IMM • 2-port 100GE CXP IMM • 2 x (48-port 10/100/1000BASE-TX MDA-XP) • 2 x (2-port OC-192c/STM-64c MDA-XP) • 2 x (16-port ATM OC-3c/STM-1c)

Tabla 3: Equipamiento y Tarjetería

En caso de necesidades futuras a largo plazo, sería necesario aumentar el número de equipos en la frontera de la red para así permitir un mayor número de accesos de clientes finales.

En cuanto a los protocolos que usaremos en la configuración del *backbone*, el cliente se decantó por el uso de OSPF como protocolo de enrutamiento IGP, y LDP como protocolo para la distribución de etiquetas de transporte MPLS.

EL uso de OSPF es una decisión muy generalizada en redes de *backbone* basadas en tecnología IP y de tamaño medio-grande. Los tiempos de convergencia son bajos, lo que agiliza los tiempos de respuesta de la red después de un fallo (aun cuando no hay habilitadas medidas de contingencia como LFA). Además suele usarse en arquitecturas

de proveedor con un núcleo de red de alta velocidad que interconecte diversos puntos de presencia, como se da en este caso.

La decisión de usar LDP viene motivada por el hecho de que en caso de migrar hacia un b*ackbone* de red mayor, con mayor número de elementos de borde o incluso con la inclusión de nodos adicionales en el núcleo, LDP responde mejor ante la escalabilidad, derivando en menores costes de planificación y gestión, y ventanas más cortas de tiempo para su configuración. Para proveedores de servicios donde el ancho de banda no es un problema gracias a su infraestructura (como el anillo de fibra ya desplegado), y donde los cuellos de botella por excesivo tráfico fluyendo en un determinado camino tampoco lo sean, al menos en un futuro a corto-medio plazo, que obliguen a desarrollar ingeniería de tráfico, LDP es una opción ampliamente utilizada.

Los direccionamientos privados utilizados en el despliegue de la solución serán los siguientes:

Nombre del Equipo	Dirección IP de Sistema (System IP Address)
PE1_POP1MadridNorte	172.24.0.1/32
PE2_POP1MadridNorte	172.24.0.2/32
P1_POP1MadridNorte	172.24.0.5/32
P2_POP1MadridNorte	172.24.0.6/32
PE3_POP2MadridSur	172.25.0.3/32
PE4_POP2MadridSur	172.25.0.4/32
P3_POP2MadridSur	172.25.0.7/32
P4_POP2MadridSur	172.25.0.8/32

Tabla 4: Tabla de direccionamiento IP para las interfaces de sistema

Conectividad entre POPs (Backbone) Nombre del Equipo – Interfaz hacia XXX	Dirección IP de la Interfaz
P1_POP1MadridNorte – Interfaz hacia P3	172.30.1.1/30
P1_POP1MadridNorte – Interfaz hacia P4	172.30.1.5/30
P2_POP1MadridNorte – Interfaz hacia P3	172.30.1.9/30
P2_POP1MadridNorte – Interfaz hacia P4	172.30.1.13/30
P3_POP2MadridSur – Interfaz hacia P1	172.30.1.2/30
P3_POP2MadridSur – Interfaz hacia P2	172.30.1.10/30
P4_POP2MadridSur – Interfaz hacia P1	172.30.1.6/30
P4_POP2MadridSur – Interfaz hacia P2	172.30.1.14/30

Tabla 6: Tabla de direccionamiento IP para la conectividad entre los POPs

Conectividad en los POPs Nombre del Equipo – Interfaz hacia XXX	Dirección IP de la Interfaz
PE1_POP1MadridNorte – Interfaz hacia P1	172.24.1.1/30
PE2_POP1MadridNorte – Interfaz hacia P2	172.24.1.5/30
P1_POP1MadridNorte – Interfaz hacia PE1	172.24.1.2/30
P2_POP1MadridNorte– Interfaz hacia PE2	172.24.1.6/30
P1_POP1MadridNorte – Interfaz hacia P2	172.24.1.9/30
P2_POP1MadridNorte– Interfaz hacia P1	172.24.1.10/30
PE3_POP2MadridSur – Interfaz hacia P3	172.25.1.1/30
PE4_POP2MadridSur – Interfaz hacia P4	172.25.1.5/30
P3_POP2MadridSur – Interfaz hacia PE3	172.25.1.2/30
P4_POP2MadridSur– Interfaz hacia PE4	172.25.1.6/30
P3_POP2MadridSur – Interfaz hacia P4	172.25.1.9/30
P4_POP2MadridSur– Interfaz hacia P3	172.25.1.10/30

Tabla 5: Tabla de direccionamiento IP para la conectividad en los POPs

4.3 Configuración de la solución

A continuación se presentaran las plantillas de configuración para desplegar la solución en los equipos de Frontera y Backbone. Se han tomado como ejemplos de configuración los siguientes equipos. En el resto de elementos se seguirán los mismos pasos a excepción de los cambios pertinentes en el nombre, direccionamiento de las interfaces, numeración de tarjetas, contraseñas.

- PE1_POP1MadridNorte
- P1_POP1MadridNorte

PE1_POP1MadridNorte:

```
# Configuración básica
configure system name PE1_POP1MadridNorte
configure system security telnet-server
configure system login-control telnet inbound-max-sessions 5
configure system security user "admin" password <clave_administrador>
configure system login-control idle-timeout 60
configure system time zone <nombre_zona>
configure system security snmp community <nombre_de_la_comunidad> rwa version
both
configure system snmp packet-size 9216
configure system snmp no shutdown

# Configuración de la tarjetería
configure card <slot_de_la_tarjeta> card-type <tipo_de_tarjeta_IOM/IMM>
configure card <slot_de_la_tarjeta> mda <1/2> <tipo_de_tarjeta_MDA>

# Configuración de la Interfaz de Sistema
configure router interface system
configure router interface system address 172.24.0.1/32
# Configuración de las Interfaces de conexión con otros nodos
configure router interface to_P1_POP1MadridNorte
configure router interface to_P1_POP1MadridNorte address 172.24.1.1/30
configure router interface to_P1_POP1MadridNorte port <puerto_x/y/z>

# Configuración de OSPF
configure router ospf area 0
configure router ospf area 0 interface system
configure router ospf area 0 interface to_P1_POP1MadridNorte interface-type
point-to-point
#Para habilitar LFA
configure router ospf loopfree-alternate

# Configuración de LDP
configure router ldp
configure router ldp interface-parameters interface to_P1_POP1MadridNorte
configure router ldp targeted-session
# Habilitar Fast Re-Route
configure router ldp fast-reroute

# Habilitamos ECMP para el balanceo de carga ante múltiples caminos de igual
# coste (bajo el mismo protocolo)
configure router ecmp 4

# Configuración MP-BGP, para las sesiones entre los enrutadores de frontera.
configure router bgp family vpn-ipv4
configure router bgp group "MP-iBGP"
```

```
configure router bgp group “MP-iBGP” peer-as 64495
configure router bgp group “MP-iBGP” neighbor 172.24.0.2
configure router bgp group “MP-iBGP” neighbor 172.24.0.3
configure router bgp group “MP-iBGP” neighbor 172.24.0.4
```

P1_POP1MadridNorte:

```
# Configuración básica
configure system name P1_POP1MadridNorte
configure system security telnet-server
configure system login-control telnet inbound-max-sessions 5
configure system security user "admin" password <clave_administrador>
configure system login-control idle-timeout 60
configure system time zone <nombre_zona>
configure system security snmp community <nombre_de_la_comunidad> rwa version
both
configure system snmp packet-size 9216
configure system snmp no shutdown

# Configuración de la tarjetería
configure card <slot_de_la_tarjeta> card-type <tipo_de_tarjeta_IOM/IMM>
configure card <slot_de_la_tarjeta> mda <1/2> <tipo_de_tarjeta_MDA>



# Configuración de la Interfaz de Sistema
configure router interface system
configure router interface system address 172.24.0.5/32

# Configuración de las Interfaces de conexión con otros nodos
configure router interface to_PE1_POP1MadridNorte
configure router interface to_PE1_POP1MadridNorte address 172.24.1.2/30
configure router interface to_PE1_POP1MadridNorte port <puerto_x/y/z>

configure router interface to_P2_POP1MadridNorte
configure router interface to_P2_POP1MadridNorte address 172.24.1.9/30
configure router interface to_P2_POP1MadridNorte port <puerto_x/y/z>

configure router interface to_P3_POP2MadridSur
configure router interface to_P3_POP2MadridSur address 172.30.1.1/30
configure router interface to_P3_POP2MadridSur port <puerto_x/y/z>

configure router interface to_P4_POP2MadridSur
configure router interface to_P4_POP2MadridSur address 172.30.1.5/30
configure router interface to_P4_POP2MadridSur port <puerto_x/y/z>

# Configuración de OSPF
configure router ospf area 0
configure router ospf area 0 interface system
configure router ospf area 0 interface to_PE1_POP1MadridNorte interface-type
point-to-point
configure router ospf area 0 interface to_P2_POP1MadridNorte interface-type
point-to-point
configure router ospf area 0 interface to_P3_POP2MadridSur interface-type
point-to-point
configure router ospf area 0 interface to_P4_POP2MadridSur interface-type
point-to-point
#Para habilitar LFA
configure router ospf loopfree-alternate
```

```
# Configuración de LDP
configure router ldp
configure router ldp interface-parameters interface to_PE1_POP1MadridNorte
configure router ldp interface-parameters interface to_P2_POP1MadridNorte
configure router ldp interface-parameters interface to_P3_POP2MadridSur
configure router ldp interface-parameters interface to_P4_POP2MadridSur
configure router ldp targeted-session

# Habilitar Fast Re-Route
configure router ldp fast-reroute

# En caso de necesitarse una política de importación o exportación, ésta
# debería de configurarse de la siguiente forma.
# Las políticas de exportación de rutas entre protocolos de enrutamiento
siguen el mismo patrón y se aplican dentro del protocolo.
configure router policy-options begin
configure router policy-options policy-statement
"nombre_politica_ldp_exportacion/importacion"
configure router policy-options policy-statement
"nombre_politica_ldp_exportacion/importacion" entry <#entrada> action
accept/reject
configure router policy-options policy-statement commit

# Aplicamos la política dentro del protocolo LDP
configure router ldp <import/export>
<nombre_politica_ldp_exportacion/importacion>

# Habilitamos ECMP para el balanceo de carga ante múltiples caminos con el
# mismo coste (bajo el mismo protocolo)
configure router ecmp 4
```

Hay que recalcar que esta configuración corresponde únicamente a los equipos de frontera y *backbone* de la solución desplegada, dejando aparte las configuraciones de los equipos ya desplegados en los POP que puedan centralizar o agregar accesos de otras tecnologías, aunque deban éstos tenerse en cuenta durante el despliegue del proyecto, pero cuya configuración llevará a cabo el departamento de TI de cliente (se tendrá en cuenta en la planificación que se detallará en el Capítulo correspondiente).

Capítulo 5: Monitorización, Gestión y Mantenimiento de la Red

5.1 Herramientas de Monitorización, Gestión y Mantenimiento.

Uno de los aspectos más relevantes en toda red de proveedor de servicios, es lo concerniente a la monitorización. Gracias a ella, se facilitan las labores de operación de los servicios y de los propios equipos. Con la implementación de un sistema de monitorización adecuado, el proveedor de servicios, en nuestro caso particular el cliente Abstractel S.A., será capaz no sólo de actuar reactivamente frente a posibles problemas dentro de su red, sino también de advertir o incluso prevenir éstos antes de que ocurran, de forma proactiva.

La práctica totalidad de herramientas de monitorización del mercado hacen uso del protocolo SNMP (*Simple Network Management Protocol*), definido en el RFC 1157 [Ref. 17]. Fue actualizado a su versión más reciente SNMPv3 en el RFC 3410 [Ref.18], que incluye cambios con respecto a las dos versiones anteriores, en su mayoría relacionados con la seguridad, pero que, sin embargo, no ha sido "aceptado" ampliamente aún por la mayoría de los fabricantes.

SNMP se basa en el uso de dos componentes principales; los Agentes y los Sistemas de Gestión de Red (NMS – *Network Management Systems*).

Un agente no es más que un software residente en el dispositivo a administrar, que tiene acceso a la información que se desea monitorizar, como por ejemplo, memoria RAM utilizada, % CPU utilizado, número de paquetes IP recibidos/enviados, ancho de banda disponible, etc. Estos agentes se encargan de organizar esa información de manera jerárquica y de asignar a cada variable de información un identificador unívoco. Estos identificadores son los denominados OIDs (*Object IDentifiers*) y al orden jerárquico en que éstos están organizados es a lo que llamamos MIB (*Management Information Database*).

El NMS por su parte, como su nombre indica, es el sistema de gestión de la red. Es el software encargado de solicitar a los agentes mediante SNMP la información de los OIDs que correspondan dentro de la MIB. El NMS no sólo puede realizar labores de "lectura" de las variables almacenadas por los agentes vía SNMP, también puede llevar a cabo labores de "escritura" de variables.
Bajo condiciones normales el NMS pide a los agentes la información necesaria para la monitorización. Existe, sin embargo, la posibilidad de que un agente envíe información al NMS sin haber sido solicitada. Este tipo de mensajes SNMP es a lo que denominamos "*Traps*", y suelen enviarse bajo ciertas condiciones de cambio, error, o como alarmas ante situaciones inesperadas.

Si bien es cierto que existen muchas y variadas herramientas para monitorización de la red, inclusive algunas de código libre, no todas cuentan con capacidades de gestión y

mantenimiento remoto del equipamiento de red. Es por ello que, siguiendo las directrices en cuanto a necesidades que precisa el cliente y teniendo en cuenta el equipamiento ya desplegado, la solución escogida ha sido el software 5620 SAM (Service Aware Manager). Éste se encuentra, de nuevo, dentro del portfolio del fabricante Alcatel-Lucent, y es una de las múltiples herramientas que propone el fabricante para la gestión integral de la red.
5620 SAM no sólo hace uso del protocolo SNMP para la interacción con los elementos de red, sino que también se apoya en protocolos como FTP (*File Transfer Protocol*) o SCP (*Secure Copy*) para la recolección y transferencia de información con el servidor principal o auxiliar de este Sistema de Gestión de Red. Incluso, llegado el caso, puede tenerse accesos al equipo mediante una sesión sobre el protocolo Telnet o SSH (*Secure Shell*) dentro de la propia herramienta.

5.2 Visión general del 5620 - *Service Aware Manager* (SAM)

Alcatel-Lucent 5620 Service Aware Manager, o 5620 SAM, permite la monitorización de elementos de red (NEs – *Network Elements*), posibilitando la gestión y el mantenimiento de redes y servicios extremo a extremo. Dichos NEs pueden ser tanto de Alcatel-Lucent como de otros fabricantes, aunque en este último caso las capacidades de gestión se vean algo más limitadas.

Nota: Los elementos de red de terceros se definen dentro del entorno de SAM como GNE (*Generic Network Elements*).

Con 5620 SAM nuestro cliente podrá realizar tareas como:

- Gestión de los servicios.
- Contabilización de Estadísticas.
- Administración y gestión del equipamiento.
- Monitorización del rendimiento.
- Solución de problemas o fallos.

La principal ventaja de esta herramienta es que permite realizar una operación eficiente e integral de entornos IP/MPLS, como el que estamos desplegando para nuestro proveedor, enfocados a la creación de servicios de interconexión. Bajo la misma plataforma, SAM ofrece herramientas muy completas para el aprovisionamiento de equipamiento, la propia configuración de los nodos, la gestión de los servicios desplegados de extremo a extremo, y la obtención de la información relevante para la elaboración de gráficas y estadísticas (ambas también disponibles en la plataforma).

Además de lo mencionado, gracias a las dependencias entre elementos que la herramienta es capaz de deducir en base a la configuración que rescata de los NEs, se dispone de una perspectiva global y relacional de los nodos que componen la arquitectura. Usando esta visión, que la herramienta puede mostrar de manera gráfica, podemos por ejemplo, simplificar y acelerar el despliegue de servicios. Por otro lado, desde el punto de vista de la solución de problemas, SAM ayuda en la mejora de los

tiempos de detección de fallos, gracias a su correlación de alarmas y sus herramientas de análisis, para dar con la causa raíz del problema.

5.3 Arquitectura del Sistema de Gestión, Monitorización y Mantenimiento

Antes de describir la arquitectura particular desplegada para nuestro cliente Abstractel S.A., se definirán a continuación los componentes típicos de una arquitectura usando el NMS 5260 SAM elegido:

- **Servidor Principal**: Es el elemento primordial como su nombre indica. Puede definirse como el motor de procesamiento de la herramienta, y está basado en lenguaje Java. Corre sobre plataformas Solaris x86 o sobre RHEL (*Red Hat Enterprise Linux*) e incluye además componentes de terceros tales como un servidor de aplicaciones, un servidor JMS (*Java Message Service*), un servidor web, etc. Algunas de sus funciones como la recolección de estadísticas pueden distribuirse y delegarse en otros servidores los cuales denominamos *auxiliares*.
- **Servidor Auxiliar**: Está también basado en Java y puede correr sobre las mismas plataformas que el principal, Solaris x86 o RHEL, pero es un componente opcional en la arquitectura. Se utiliza para dotar al entorno de mayor escalabilidad a la hora de recolectar estadísticas y *call-traces* de los elementos de red. Estos servidores están controlados por el servidor principal y recogen la información directamente de los elementos de red para almacenarla en la base de datos de SAM.
- **Bases de datos**: Esta base de datos del 5620 SAM es de tipo relacional personalizada para este entorno y proporciona almacenamiento persistente actuando como repositorio central de la información que poseemos de la red. Ésta puede localizarse en la misma máquina que el servidor principal o en una aparte, y suele desplegarse igualmente en plataformas Solaris x86 o RHEL.
- **Clientes GUI** (*Graphical User Interface*): Es un software de instalación que hace las veces de interfaz gráfica para los operadores de red, o personal que haya de realizar labores OAM. También está basado en Java y puede desplegarse en multitud de plataformas, que no tienen que coincidir con la usada en el servidor principal.
- **Clientes OSS**: Es una aplicación software desarrollada para automatizar tareas o recoger información para su posterior procesamiento. Estos clientes OSS pueden ser de diversos tipos, desde un simple script de CLI a una aplicación de terceros que interactúe con SAM. Las plataformas donde alojar estos clientes no han de ser las mismas necesariamente que las usadas en los servidores del 5260 SAM, puesto que sólo interactuarán con éstos a través de mensajes Java.

La comunicación entre los componentes de la arquitectura puede resumirse en la Figura 47, en la que podemos advertir cómo las interacciones hacen uso de protocolos estandarizados.

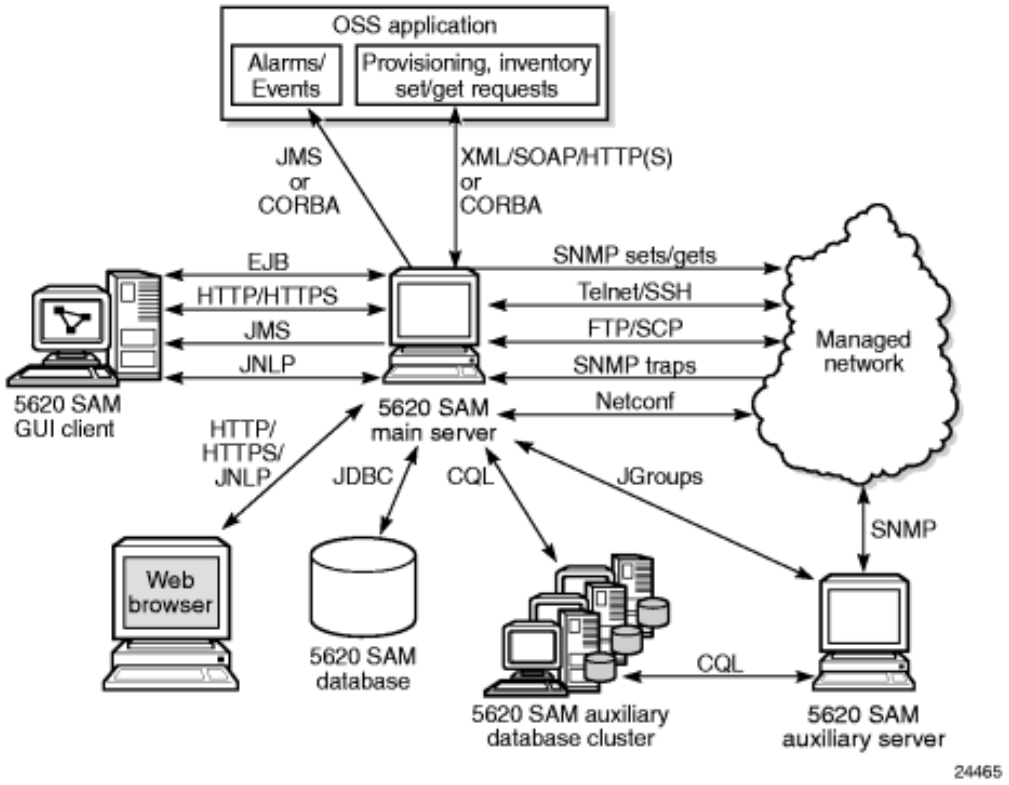


Figura 47: Comunicación entre los diversos componentes de la arquitectura [Ref. 19]

Para nuestro cliente Abstractel S.A. la solución escogida para el entorno del Sistema de Gestión, Monitorización y Mantenimiento, estará compuesta por los siguientes elementos:

- Un servidor principal
- Una base de datos
- Clientes GUI

Se ha optado por utilizar un único servidor para alojar el 5620 SAM *Main Server* y la base de datos Oracle personalizada que éste usará para alojar la información de manera centralizada.

Con la ayuda del fabricante y teniendo en cuenta las demandas de cliente (su previsión de un posible crecimiento del negocio), la opción elegida será un HPE ProLiant DL380 Gen9 Performance - 2.3 GHz - 32 GB RAM. Éste será emplazado en uno de los racks del POP 1 Madrid Norte (2U de espacio), lo que facilitará el cableado del equipo a la red. Alojará la plataforma *Red Hat Enterprise Linux Server* para 32/64-bits x86 (con un año de suscripción *Premium*, que incluye el soporte extendido de actualizaciones) como Sistema Operativo de base.

Ya que los elementos de red han de ser alcanzables por el NMS, y dado que necesitamos de una IP que esté accesible sin que ésta esté vinculada a ninguna interfaz física que pudiera incurrir en fallos, podríamos configurar una interfaz de *loopback* para tal efecto.

Sin embargo, aunque la configuración de la interfaz no sería un problema, se ha optado por utilizar la propia *System IP interface*, ya mencionada anteriormente (y utilizada por otros protocolos como el de encaminamiento), para llevar a cabo el acceso a los equipos y las peticiones SNMP por parte de la herramienta 5620 SAM.

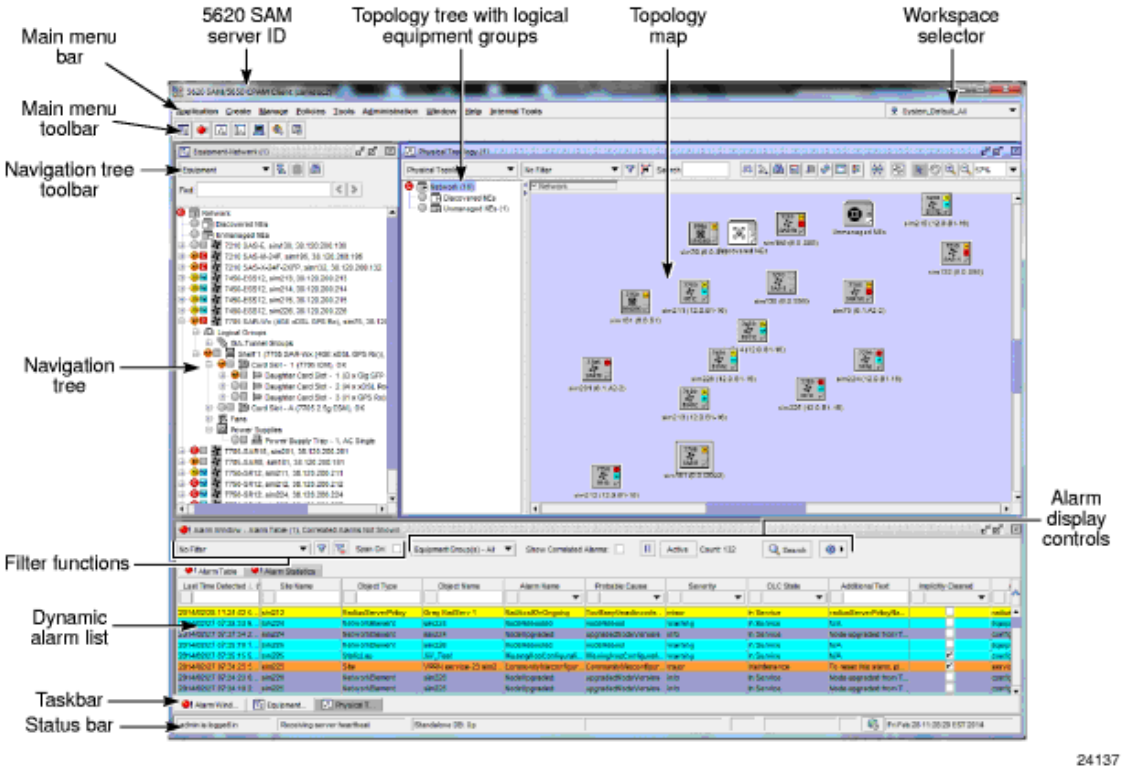
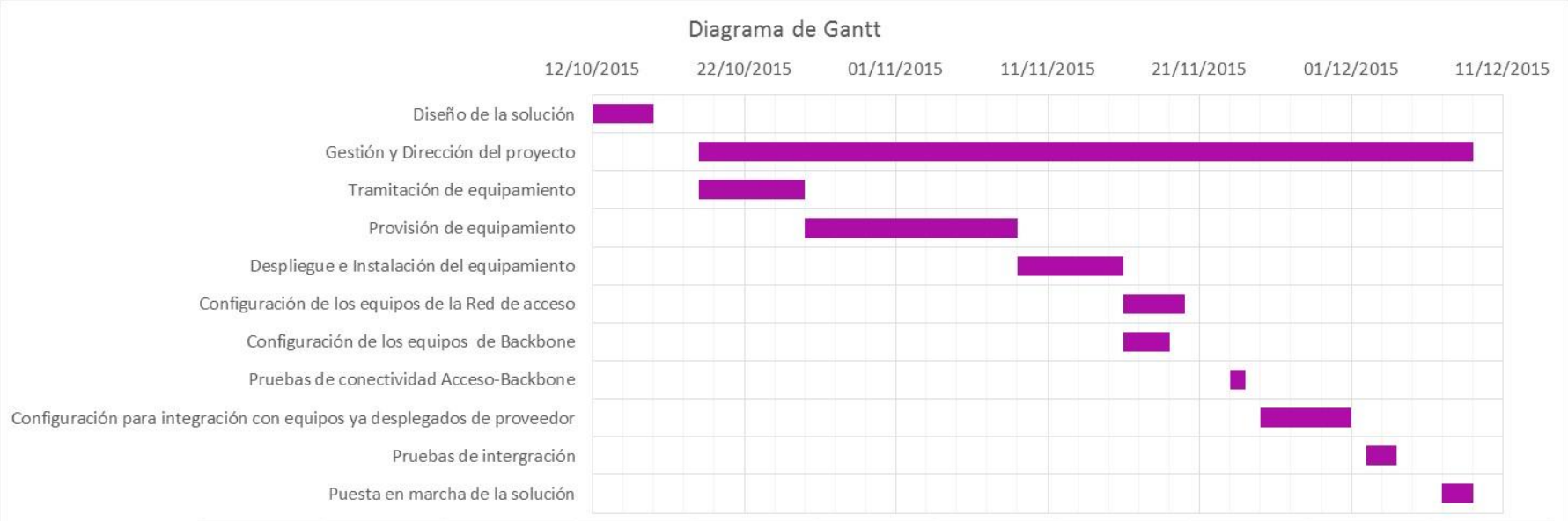


Figura 48: SAM Service Aware Manager [Ref. 20]

Capítulo 6: Presupuesto y planificación de trabajo

6.1 Planificación de trabajo – Diagrama de Gantt

La planificación de trabajo para el presente proyecto se detallará mediante el siguiente Diagrama de Gantt que muestra el tiempo de dedicación previsto para el desarrollo de las diferentes tareas en la elaboración del proyecto. El horario laboral acordado con cliente se definió en jornadas de Lunes a Viernes en horario de 9:00 AM a 6:00 PM (con una hora de descanso para la comida).



	Puesta en marcha de la solución	Pruebas de intergración	Configuración para integración con equipos ya desplegados de proveedor	Pruebas de conectividad Acceso-Backbone	Configuración de los equipos de Backbone	Configuración de los equipos de la Red de acceso	Despliegue e Instalación del equipamiento	Provisión de equipamiento	Tramitación de equipamiento	Gestión y Dirección del proyecto	Diseño de la solución
Fecha de Inicio de Tarea	07/12/2015	02/12/2015	25/11/2015	23/11/2015	16/11/2015	16/11/2015	09/11/2015	26/10/2015	19/10/2015	19/10/2015	12/10/2015
Duración	2	2	6	1	3	4	7	14	7	51	4

Tabla 7: Diagrama de Gantt - Planificación

6.2 Recursos Humanos

En primer lugar detallaremos el personal humano necesario para el despliegue del proyecto, tanto en la parte de diseño, gestión y tramitación/logística, como en las tareas de despliegue, configuración y pruebas.

Tarea/Actividad	Personal	Dedicación (Horas)	Coste (€)
Diseño y desarrollo del proyecto técnico	Arquitecto de Red	40 (8h/día)	3600
Gestión y dirección de la solución	Jefe de Proyecto	152 (4h/día)	12160
Tramitación de equipamiento e interlocución con logística	Técnico Administrativo	8 (1h/día)	480
Transporte y montaje/instalación del equipamiento	Empresa de logística/montaje especializada	XXX (no aplica)	2050
Configuración de equipos y pruebas de conectividad	2 Técnicos de red	20 (4h/día)	2600
Pruebas de integración y puesta en marcha de la solución	Administrador de red	32 (8h/día)	2240
		Coste Total	**23130**

Tabla 8: Tabla Costes asociados a Recursos Humanos

6.3 Costes de Equipamiento, Formación y Soporte

En la siguiente tabla se resumen los costes del equipamiento adquirido en propiedad por el cliente (véase apartado 4.2 Implementación y 5.3 Arquitectura del Sistema de Gestión, Monitorización y Mantenimiento). Hemos de subrayar que los precios aquí expuestos corresponden al pago a través de nuestra empresa (socio autorizado de Alcatel-Lucent) por lo que los precios unitarios llevan incluido el correspondiente descuento (función de la categoría de socio). Mencionar que en dichos costes también se detalla la inclusión de un paquete de formación, para el aprendizaje del personal TI de cliente que operará sobre los equipos, compuesto por un total de 24 personas.

También se firmó con cliente un contrato de soporte (nivel 3) con nuestra empresa, por un periodo, prorrogable, de 4 años (incluirá 1 Administrador de Red y 3 Técnicos de red en 24x7), para el caso de incidencias críticas y gestión de cambios. El pago en referencia al contrato de soporte se realizará de manera mensual, aplicándose una tarifa excepcional por la no exclusiva dedicación del personal al cliente.
Los cambios de tarjetería y actualización de software se cobrarán aparte, aunque con un descuento acordado sobre el precio de venta habitual del 45% durante los 4 primeros años tras la puesta en marcha, desplazamiento y montaje incluido.

Nota: También se ofertó por nuestra parte al cliente la posibilidad de firmar un contrato de "*renting*" (alquiler mensual) del equipamiento durante un periodo de 4 años (igualmente prorrogable), que incluía actualización o renovación y mantenimiento integral, pero finalmente el cliente rechazó la propuesta ya que en ésta se incluía una cláusula de exclusividad de equipamiento (marca) en el Backbone y frontera de red, lo cual no encajaba en sus expectativas de desarrollo de negocio, a medio-largo plazo.

Concepto	Unidades	Precio Unidad (€)	Coste (€)
Equipo Alcatel-Lucent 7750 SR-12 (tarjetería incluida)	4	80500	322000
Equipo Alcatel-Lucent 7750 SR-7 (tarjetería incluida)	4	60100	240400
Servidor HPE ProLiant DL380 Gen9 Performance	1	4500	4500
Red Hat Enterprise Linux Server 32/64-bit x86 (*Premium Subscription*)	1	1500	1500
5620 SAM Software + Licencias	1	9300	9300
Paquete de formación	3 (Grupos de 8 participantes)	8000	24000
		Coste Total	**601700**
		Coste Mensual Soporte Nivel 3	**6500**

Tabla 9: Tabla Equipamiento, Formación y Soporte

6.4 Costes indirectos derivados del despliegue

En este punto se listarán los costes derivados del desarrollo de las tareas destinadas al despliegue del proyecto durante el trascurso del mismo. Dentro de este apartado se han tenido en cuenta conceptos como el precio de las líneas móviles del Arquitecto de la solución, Jefe de Proyecto y encargado de la tramitación, gastos de locomoción por desplazamiento del personal a instalaciones de cliente y material de oficina.

Concepto	Coste (€)
Líneas Móviles e Internet	300
Locomoción	210
Material de Oficina	80
Coste Total	**590**

Tabla 10: Tabla Costes Indirectos derivados del despliegue

6.5 Coste Total del despliegue

A continuación se resumirán los cotes anteriormente desglosados que dan como resultado el coste total del despliegue de este proyecto. También se define el pago mensual derivado de contrato de Soporte.

Concepto	Coste (€)
Recursos Humanos	23130
Equipamiento + Formación	601700
Coste Indirectos	590
Coste Total	**625420**
Cuota Mensual (Soporte)	**6500**

Tabla 11: Tabla Coste Total del despliegue

Capítulo 7: Conclusiones y líneas de mejora futuras

7.1 Conclusiones

La meta de este proyecto ha sido el diseño y despliegue de una red IP/MPLS para un proveedor de servicios llamado AbstracTel S.A.

Se han tenido en cuenta para ello las directrices marcadas por el cliente, que incluían la reutilización de equipamiento y cableado ya desplegado, derivado de las actividades y dedicaciones previas de la propia empresa, para garantizar un abaratamiento en los costes.

Otro punto clave a tratar fue el posible aumento del negocio. Se diseñó la arquitectura pensando en futuras ampliaciones del equipamiento y dimensionando los elementos con la suficiente capacidad para hacer frente a los clientes actuales previstos y a los potenciales a medio-largo plazo. Así mismo, se incluyeron enlaces alternativos dentro de la solución que ayudasen a la arquitectura a reponerse ante fallos que pudieran surgir en los nodos o enlaces.

En cuanto a los protocolos utilizados durante el despliegue, se decidió con el cliente el uso de aquellos actualmente en tendencia para redes similares. Así, se utilizó OSPF como protocolo de encaminamiento (IGP) para la arquitectura del *backbone*, y que sirviera de apoyo para otros protocolos y herramientas implementados en el despliegue. Uno de los protocolos que hace uso de la topología lógica definida por el IGP, es el protocolo LDP de distribución de etiquetas MPLS, del cual se hizo uso justificado al responder éste mejor ante necesidades de escalabilidad, derivando, como ya se argumentó, en menores costes de planificación y gestión y en ventanas más cortas de tiempo para su configuración.

De igual forma, el cliente demandaba una herramienta de gestión, que le permitiera monitorizar el estado de su red, acometer tareas de mantenimiento y actualización, o inclusive, que sirviera de repositorio central/*backup* de la información. Se optó así por el sistema de gestión de red 5620 SAM de Alcatel-Lucent, que cubría las demandas expuestas y que gestiona a la perfección otro de los puntos importantes para un ISP como es el diagnóstico y solución de fallos.

7.2 Líneas de mejora futuras para la presente solución

Una de las líneas futuras de mejora pasaría por la propia ampliación de la arquitectura. A largo plazo, y en función de la cantidad de clientes, cabría la posibilidad de desplegar otro(s) POP(s) que ofrecieran cobertura a empresas situadas en otras comunidades autónomas.

A la vista de la gran variedad de servicios de interconexión que pueden implementarse con la infraestructura desplegada, el cliente podría decidirse por el uso de RSVP-TE como protocolo de distribución de etiquetas. Es de gran utilidad si las capacidades de la red y el dimensionamiento de enlaces *se ven limitados* por el gran número de clientes finales. En este caso la ingeniería de tráfico que ofrece este protocolo, permite por ejemplo la reserva de recursos (anchos de banda en los enlaces para según qué tipo de tráfico), el uso de *paths* definidos administrativamente en los LSPs, la posibilidad de desviar el tráfico a caminos alternativos predefinidos en caso de fallos, etc.

Como ya se mencionó, los servicios de interconexión tipo VPN hoy en día son uno de los más ampliamente utilizados por las corporaciones para el intercambio de información y comunicaciones entre sus sedes distantes geográficamente. La naturaleza del tráfico intercambiado entre sedes de una misma empresa puede ser muy diverso; datos entre aplicaciones corporativas o correos electrónicos, llamadas telefónicas digitalizadas que hacen uso del transporte sobre redes de paquetes (VoIP), video-llamadas en tiempo real, *streaming* de video, etc. Todas estas clases de tráfico pueden viajar a través de la red del ISP, y mientras no existan problemas de congestión y el volumen de tráfico no sea elevado, no habrá problemas en los tratamientos. Ahora bien, si los enlaces comienzan a saturarse, como es comprensible, tráficos de diferente naturaleza, necesitan tratamiento de distinta índole. Y será entonces cuando nuestro cliente AbstracTel S.A. pueda decidir mejorar este tratamiento del tráfico, definiendo nuevas políticas de Calidades de servicios (QoS - Quality of Service) en los nodos de red, que se ajusten más a las necesidades de sus clientes finales.

Bibliografía

[Ref. 1 y 2] RFC 3031. Multiprotocol Label Switching Architecture. Enero 2001.

[Ref. 3] RFC 4447. Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP). Abril 2006.

[Ref. 4 y 9] RFC 4364. BGP/MPLS IP Virtual Private Networks (VPNs). Febrero 2006.

[Ref. 5] RFC 3032. MPLS Label Stack Encoding. Enero 2001.

[Ref. 6] RFC 4182. Removing a Restriction on the use of MPLS Explicit NULL. Septiembre 2005.

[Ref. 7] RFC 3036. LDP Specification. Enero 2001.

[Ref. 8] RFC 5036. LDP Specification. Octubre 2007.

[Ref. 9 y 4] RFC 4364. BGP/MPLS IP Virtual Private Networks (VPNs). Febrero 2006.

[Ref. 10] RFC 2547bis (Internet-Draft). BGP/MPLS IP VPNs. Octubre 2004.

[Ref. 11] Alcatel-Lucent. 7750 Service Routers.

https://www.alcatel-lucent.com/products/7750-service-router

[Ref. 12] Alcatel-Lucent. 7750 Service Routers. Mobile Gateway.

https://www.alcatel-lucent.com/products/7750-service-router-mobile-gateway

[Ref. 13, 14, 15 y 16] Alcatel-Lucent. 7750 Service Routers. Related Materials. Datasheets.

https://www.alcatel-lucent.com/products/7750-service-router

[Ref. 17] RFC 1157. A Simple Network Management Protocol (SNMP). Mayo 1990.

[Ref. 18] RFC 3410. Introduction and Applicability Statements for Internet Standard Management Framework. Diciembre 2002

[Ref. 19] Alcatel-Lucent. 5620 SAM Service Aware Manager.

https://www.alcatel-lucent.com/products/5620-service-aware-manager

[Ref. 20] Alcatel-Lucent. 5620 SAM Service Aware Manager.

https://infocenter.alcatel-lucent.com/public/5620SAM120R5A/index.jsp?topic=%2FSAM_UG%2Fhtml%2Fsam_about_gui.html